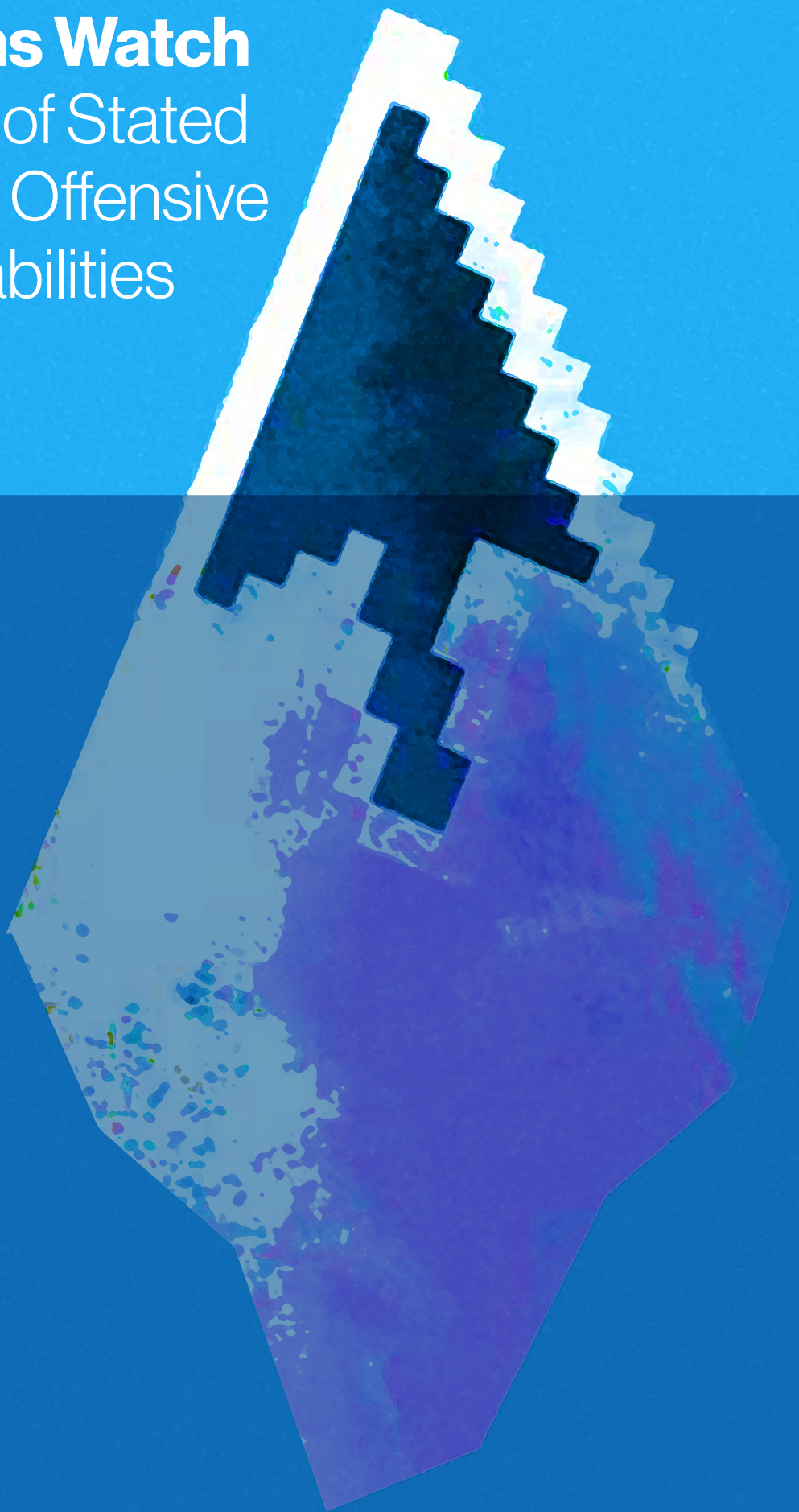
The Hague Centre
for Strategic Studies

Cyber Arms Watch

An Analysis of Stated & Perceived Offensive Cyber Capabilities

May 2022



The Hague Centre
for Strategic Studies

The Cyber Arms Watch

Uncovering the Stated & Perceived Offensive Cyber Capabilities of States

Project Team:
Louk Faesen, Alexander Klimburg (former Cyber Program Director at HCSS), Michel Rademaker and Saskia Heyster

Assistant Analysts:
Simon van Hoeve, Raffaele Minicozzi, Salome Petit Siemens and Giulia Tesauro

ISBN/EAN: 9789083254111
May 2022

The research for and production of this report has been conducted with support of the Municipality of The Hague. Responsibility for the contents and for the opinions expressed, rests solely with the authors and does not constitute, nor should be construed as, an endorsement by the Municipality.

Table of Contents

1. **Rationale:** A lack of Transparency

Conflict between states has taken on new forms, and cyber operations play a leading role in this increasingly volatile environment, earning them a top spot among states' most critical security concerns. According to the Council on Foreign Relations, 34 states are suspected of sponsoring cyber operations since 2005.[1] Despite the high level of activity, relatively little is publicly known about the offensive cyber capabilities of states. This is despite the widely held concern in diplomatic circles that tensions in cyberspace are escalating, and the likelihood of a catastrophic cyber exchange between nation states continues to rise. Such a calamity could well happen by accident. Avoiding "inadvertent escalation" – or accidental war – remains the most significant challenge between states in cyberspace.

Despite the high level of activity, relatively little is publicly known about the offensive cyber capabilities of states.

A major contribution to this uncertainty is the lack of transparency of offensive cyber capabilities. Unlike other military systems, they are largely treated as dark secrets from the espionage world. Traditional arms control efforts have depended upon the ability to count weapon systems, like tanks and missiles, to regulate their deployment. But there is no common understanding of what "cyber weapons" are, or indeed even "cyber forces". States are left guessing as to the overall capability of another state (albeit at widely varying degrees of detail) without, for the most part, being able to detail the exact order of battle, table of equipment, tactics, techniques, procedures or other basic information – unless the intelligence assessment is very complete.[2] This secrecy has implications not only for intelligence and national security assessments, but more so for both the institutional dialogues and the wider public discussion on international peace and security in cyberspace, by foreclosing any common language on offensive cyber capabilities and intent.

Because of the lack of transparency, intergovernmental, track 1 and track 2 discussions often lack any basis for common exchange. It frustrates meaningful progress for predictability, confidence-building measures (e.g. within regional organisations such as ASEAN and the OSCE), norms of responsible state behaviour (e.g. within the United Nations), and other stability measures. The lack of transparency also impacts and limits the wider public discussion: the general absence of information means that much of the public, media, and academic discussion is not in sync with reality and risks becoming irrelevant.

1 Council of Foreign Relations, "Cyber Operations Tracker", last accessed in May 2022.

2 Alexander Klimburg and Louk Faesen, "Balance of Power in Cyberspace," in Dennis Broeders and Bibi van den Berg (ed.), "Governing Cyberspace: Behavior, Power, and Diplomacy" (2020).

2. **Objective:** A Cyber Transparency Index

The Cyber Arms Watch aims to make a contribution to international peace and security by developing the first iteration of a "Cyber Transparency Index" that offers insight into the stated and the perceived offensive cyber capabilities of 60 states. Inspired by the Freedom House Index, the results are visualized as an interactive world map monitor, offering diplomats, academics and researchers alike full access to the underlying database.

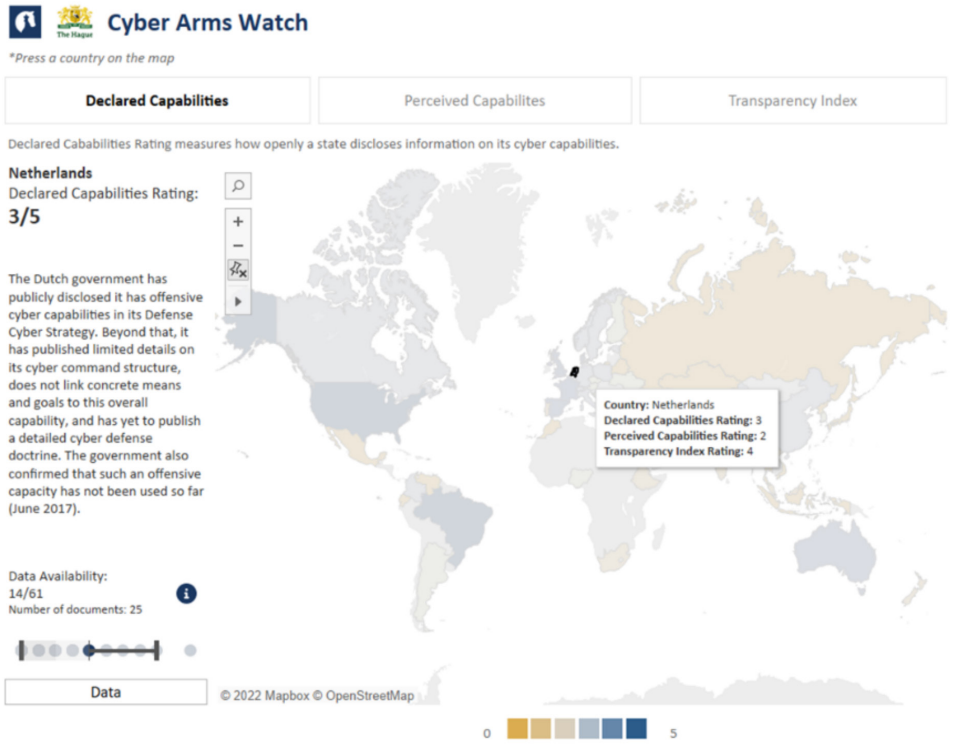
The Cyber Arms Watch offers insight into the current state of transparency in offensive cyber capabilities. Academic research has shown time and time again that transparency on "new weapons" helps reduce the scope for misunderstanding, provides for clarity of intent and predictability, and helps establish norms of restraint and communication – all essential ingredients for stability. Finally, more transparency would bring many of the public, media, and academic discussions closer to reality.

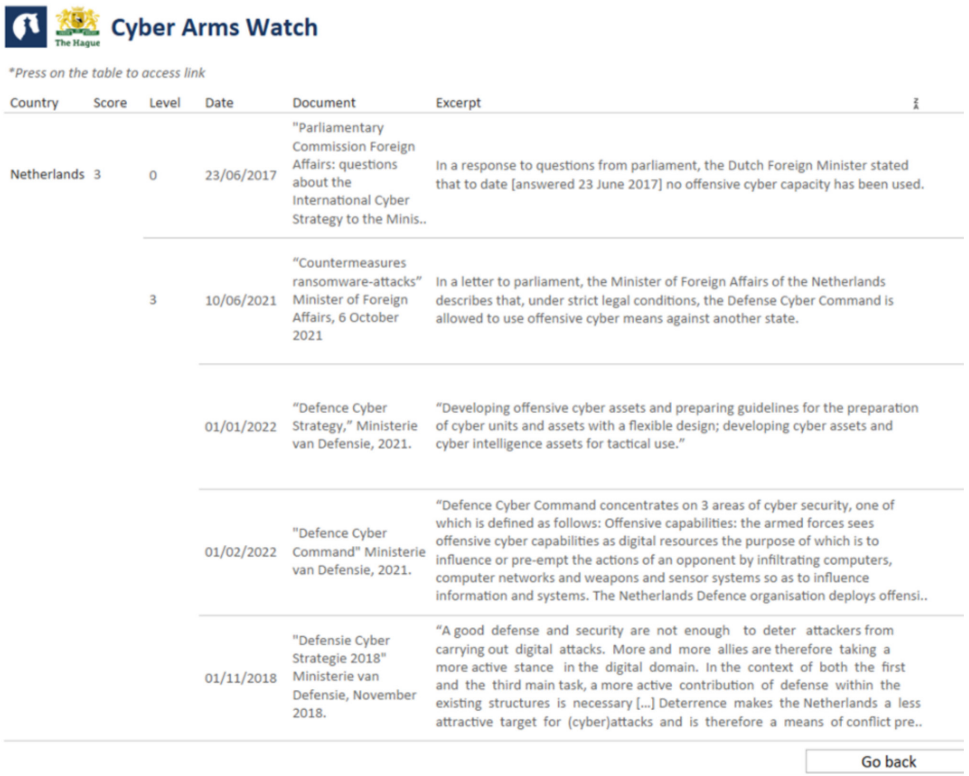
3. **Introducing** the Cyber Arms Watch Monitor

The Cyber Arms Watch is visualized as an interactive monitor with three tabs: (1) Declared Capabilities, (2) Perceived Capabilities, (3) Transparency Index.

Each country is assigned a colour contingent on the overall scoring of the given rating, with the colour scale demarcated across the bottom of the monitor.[3] By clicking on a country, the associated country level score and analysis is generated by the monitor and displayed on the left of the page. The declared capabilities and perceived capabilities ratings also include a data availability ranking that ranks the countries from 1 to 60 (1 representing the largest dataset, 60 the lowest) being based on the number of sources found that country and a boxplot of sample counts. Hovering over a country generates a box indicating the country and its associated rating.

At the bottom of each page, there is a "Data" button, which the user can click to access the sources on which the rating of the country is based on. This prompts a table of the data sources categorized on the basis of a specific score, the date of publication, the name of the document and the excerpt justifying its score. When clicking on the excerpt, the user will be redirected to the Internet page of the respective source.





3 Note that the colour scale between DCR, PCR and Transparency pages of the dashboard are different. This is because the nature of the data has slight contrasts. DCR and PCR receive a value on a numeric scale between 0-5, whilst transparency is measured using categorical labels. For ease of understanding by the user, this divergence is reflected in the colour scale.

4. **Methodology** and Results

4.1. The Cyber Transparency Index

In its methodology, the Cyber Arms Watch offers a novel proposal for assessing how transparent states are about their offensive cyber capabilities and compares this to their perceived capabilities. It enables the determination of an overall "Cyber Transparency Index" for states by using two specific ratings:

- **The Declared Capabilities Rating (DCR)** indicates to what extent a state publicly discloses information about its offensive cyber capabilities. This includes official communication by the respective government, such as strategies, doctrines, and similar documents, as well as sanctioned media reporting that cumulatively indicate the level of declared capability using a six-tiered labelling system (see Table 2). The classification ranges from no official indications of offensive cyber capabilities, to stated aspirations, sanctioned reporting by media or official statements, and finally a three-tiered level of official disclosures on its offensive cyber programme.

- **The Perceived Capabilities Rating (PCR)** indicates the perceived offensive cyber capabilities of a state using open-source information and categorizes them using a similar six-level categorization system. Whereas the first rating is limited to official disclosures by the respective government itself, the second rating uses external sources to show how their offensive cyber capabilities are observed by outsiders. This includes sources such as intelligence reports and assessments from other governments or non-state actors, indictments, sanctions, past operations, leaked documents.

- **The Cyber Transparency Index** is the delta between the DCR and PCR. We provide both a hard number and transparency labels that cluster nations together to describe the openness of a state in discussing its cyber capabilities (see Table 1).

Dichotomies were drawn in awarding labels to the degree of transparency exhibited by a state: firstly, the delta between DRC and PCR, and secondly, the maturity of their capabilities. Noting the size of the delta between DCR and PCR represents transparency. For example, in the case of the United States, with a DCR of 5 and PCR of 5, the delta is equal to 0 and indicates transparency. However, the condition of equality should be differently understood between states. Japan has a DCR of 0 and PCR of 0, so also has a delta of 0. Whilst both the United States and Japan have a 0 delta, these states have diverging cyber capabilities. Therefore, an additional condition for segmentation has been introduced – a distinction between high and low capabilities. This draws a representative distinction between the transparency attributed to states which receive similar transparency scores, but have different capability levels.

The reason behind the two-fold approach of a DCR and PCR is that a lack of declared capabilities does not automatically mean that such a capability is lacking. Indeed, several nations have conducted offensive cyber operations, whilst refraining from openly discussing cyber capabilities, criticizing this as a needless militarization of an otherwise peaceful domain. A lack in declared capabilities should, therefore, not always be confused with a lack of offensive programs or operations. The PCR was therefore introduced to contextualize the declared capabilities and compare them to outside observations.

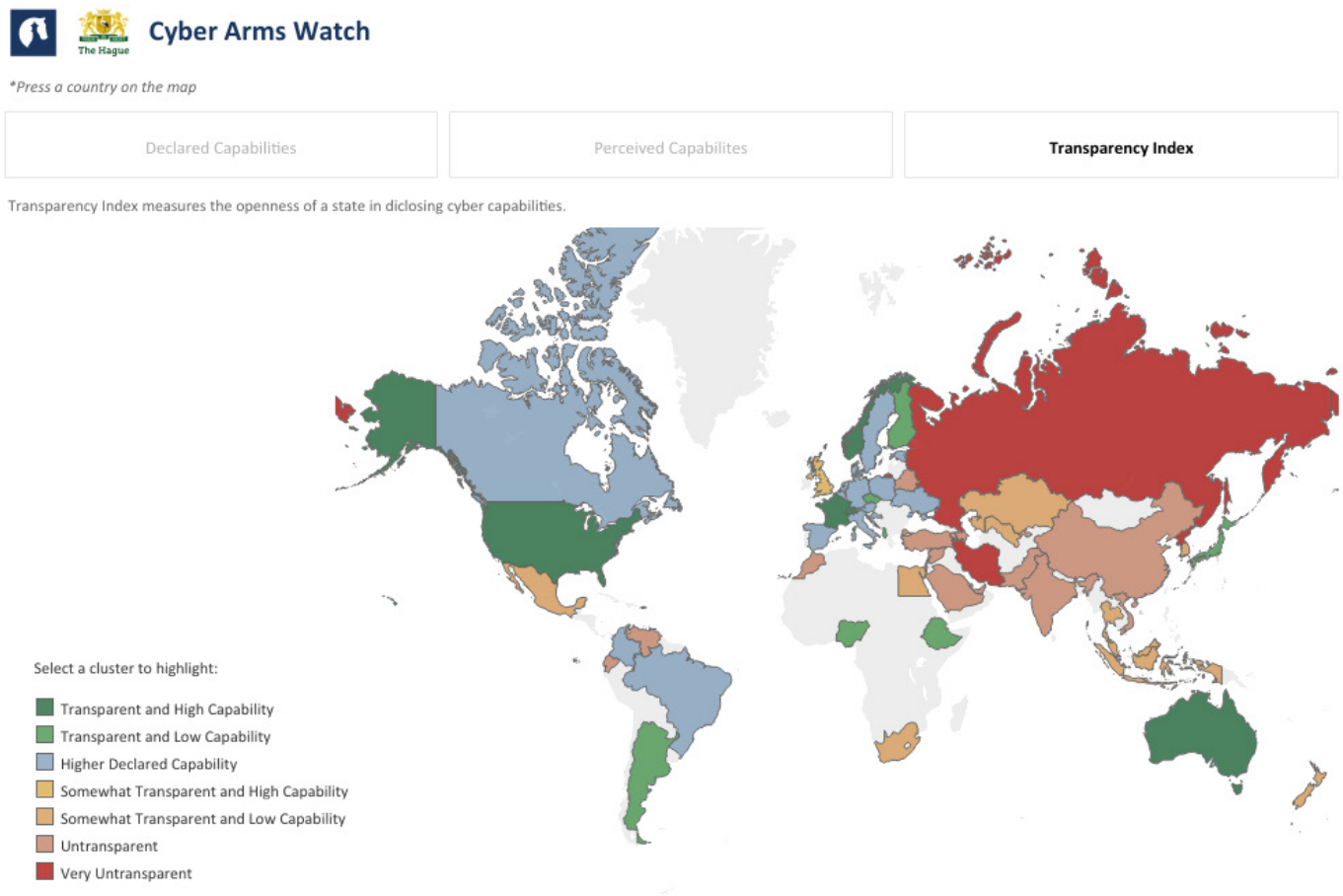
Table 1. Results of the Cyber Transparency Index

Country	DCR	PCR	Delta	Label
Democratic People's Republic of Korea	0	5	-5	Very Untransparent
Iran	0	5	-5	Very Untransparent
Russia	0	5	-5	Very Untransparent
United Arab Emirates	0	3,5	-3,5	Untransparent
Armenia	0	3	-3	Untransparent
Azerbaijan	0	3	-3	Untransparent
Belarus	0	3	-3	Untransparent
Pakistan	0	3	-3	Untransparent
Syria	0	3	-3	Untransparent
Turkey	0	3	-3	Untransparent
Vietnam	0	3	-3	Untransparent
China	3	5	-2	Untransparent
Ecuador	0	2	-2	Untransparent
India	1	3	-2	Untransparent
Israel	3	5	-2	Untransparent
Lebanon	0	2	-2	Untransparent
Morocco	0	2	-2	Untransparent
Qatar	0	2	-2	Untransparent
Saudi Arabia	1	3	-2	Untransparent
Venezuela	0	2	-2	Untransparent
Kazakhstan	0	1,5	-1,5	Somewhat Transparent and Low Capability
Bahrain	0	1	-1	Somewhat Transparent and Low Capability
Egypt	0	1	-1	Somewhat Transparent and Low Capability
Indonesia	0	1	-1	Somewhat Transparent and Low Capability
Malaysia	1	2	-1	Somewhat Transparent and Low Capability
Mexico	0	1	-1	Somewhat Transparent and Low Capability

Table 1. Results of the Cyber Transparency Index (continued)

Country	DCR	PCR	Delta	Label
New Zealand	1	2	-1	Somewhat Transparent and Low Capability
Singapore	1	2	-1	Somewhat Transparent and Low Capability
South Africa	1	2	-1	Somewhat Transparent and Low Capability
South Korea	2	3	-1	Somewhat Transparent and Low Capability
Thailand	0	1	-1	Somewhat Transparent and Low Capability
Uzbekistan	0	1	-1	Somewhat Transparent and Low Capability
United Kingdom	4	5	-1	Somewhat Transparent and High Capability
Albania	0	0	0	Transparent and Low Capability
Argentina	2	2	0	Transparent and Low Capability
Finland	2	2	0	Transparent and Low Capability
Nigeria	2	2	0	Transparent and Low Capability
Czech Republic	2	2	0	Transparent and Low Capability
Australia	4	4	0	Transparent and High Capability
France	4	4	0	Transparent and High Capability
Norway	3	3	0	Transparent and High Capability
Switzerland	3	3	0	Transparent and High Capability
United States	5	5	0	Transparent and High Capability
Austria	3	2	0	Higher Declared Capability
Canada	3	2,5	0,5	Higher Declared Capability
Estonia	3,5	3	0,5	Higher Declared Capability
Belgium	3	2	1	Higher Declared Capability
Colombia	3	2	1	Higher Declared Capability
Croatia	1	0	1	Higher Declared Capability
Germany	3	2	1	Higher Declared Capability
Italy	3	2	1	Higher Declared Capability
Netherlands	3	2	1	Higher Declared Capability
Poland	3	2	1	Higher Declared Capability
Sweden	3	2	1	Higher Declared Capability
Denmark	4,5	3	1,5	Higher Declared Capability
Brazil	5	3	2	Higher Declared Capability
Spain	4	2	2	Higher Declared Capability
Ukraine	2	0	2	Higher Declared Capability

Image 1. Visualization of the results of the Cyber Transparency Index



4.2. **Finding and Labelling Sources**

The data underpinning our analysis was gathered through research of published materials and in some cases complemented by expert interviews. A guideline was adopted for the selection of sources. For the declared capabilities, only official government documents and sanctioned media reporting are considered. This includes government strategies, military doctrines, field manuals, legislation, press releases, official websites of cyber commands or similar government entities in charge of offensive cyber, official communication from the executive branch to inform parliament, interviews with government officials or publications by government officials. For the perceived capabilities, source selection extended to open-source information found outside of the respective government's channels. This includes both state and non-state sources, such as public attributions, indictments, sanctions, intelligence reports from other nations, industry reports and attributions, news articles from media outlets, academic sources or think tank reports.

To find relevant sources, a series of related keywords were compiled around offensive cyber capabilities and applied to the search terms. This includes a generic bucket used to describe offensive cyber capabilities, such as "offensive cyber operation", "advanced persistent threat",

"cyber weapon", "active defence", "cyber warfare", "cyber and electromagnetic activity", "computer network attack", "computer network operation", "cyber command", etc. In addition, a country-specific bucket was applied to refine the search terms, which was particularly useful for non-Anglo-Saxon countries. These include keywords in the respective language, such as the "name of the cyber command", "name of the intelligence agencies", "offensive cyber operation translated into respective language".

We sought to limit the number of source that describe an event to one. For example, while there are hundreds of sources that describe Stuxnet or WannaCry, we would only include one source (e.g. a public attribution) unless a different source category (e.g. an indictment or an academic source) provides additional information.

The labelling system of the Cyber Arms Watch signifies a first iteration of a transparency assessment that can lay the groundwork for further examination and analysis. It is obviously just one simple approach that need not frame a "final answer". But it may form a beginning that can be further finetuned or expanded upon. The methodology for compiling the underlying database relies on the labelling of publicly available sources according to a six-tiered categorization system for both ratings (see Table 2). Each source is labelled individually and taken together constitute the overall country score for both the declared and perceived capabilities rating. In other words, the DCR and PCR score for each country is based on the highest-ranked source.

The cyber capabilities discussed here cover the wider gamut of cyber operations, primarily focusing on cyber effect operations from Level 3 onwards in the perceived capability rating (PCR). For these operations, we particularly look at strategic cyber capabilities, which largely uses conventional Internet technologies or even the Internet itself, and are often marked by a much slower operational tempo in multi-use computer networks (often associated with Advanced Persistent Threats) than tactical or battlefield cyber capabilities. The latter is sometimes called Cyber Electro-Magnetic Activities (CEMA) and is still included in the database, just like cyber-enabled influence operations. From Level 3 onwards, offensive cyber capabilities that deliver effects are differentiated in terms of their effects and scale.

Table 2. The six-tiered labelling system for the Cyber Arms Watch

Label	Declared Capabilities Rating (DCR)	Perceived Capabilities Rating (PCR)
Level 0	No Official Indications of Offensive Cyber Capability	No aspirations to obtain offensive cyber capabilities
Level 1	Stated Aspiration for Offensive Cyber Capability	Perceived to have obtained or used spyware capabilities.
Level 2	Sanctioned media reporting on offensive cyber details and/or operations by an official (capabilities likely to exist but unconfirmed by official resources, the extent of which being unknown)	Perceived to be working on obtaining offensive cyber capabilities
Level 3	National strategy or related official document mentioning existing offensive cyber capabilities	Perceived to have either launched or obtained the ability to launch some forms of cyber effect operation
Level 4	Defence cyber strategy or similar with details on offensive cyber command structures (general order of battle) and missions, conditions of employment and overall principles of operation	Perceived to have integrated offensive cyber capabilities into their military structure and use it (either literally or as a deterrent) to achieve strategic objectives.
Level 5	Defence cyber strategy or similar where offensive cyber capabilities are detailed, including available definitions of different types of cyber effects, detailed order of battle (units, manpower, budget), as well as specific and general TTPs.	Viewed as having launched several successful offensive cyber effect operations, with the proven capability to denigrate and destroy enemy systems or infrastructure.

Prior to Level 3 of cyber effect capabilities and operations, the monitor also includes cyber-enabled intelligence and surveillance operations in the perceived capability rating. While this is not widely considered to be an offensive cyber effect, its inclusion was considered relevant because it often functions as a precursor for cyberattacks or can be indicative of a nascent cyber capability.

Overall, a source is included in the database when it can be labelled as Level 1 or higher. From that point they contribute to both the declared and perceived capability rating. On an exceptional basis, sources with a Level 0 or n/a labels are included in the database because they offer context but do not weigh in on the country scores. Overall, the underlying reasons for their inclusion usually can be attributed to the following four reasons. First, ambiguous terminology is used that vaguely hints at an offensive capability, but cannot be labelled as such because it is not explicit enough (e.g. proactive response). Second, a lack of sources with a Level 1 and higher score were found so Level 0 documents were included to offer context (e.g. Japan's pacifist constitution). Third, reference to other indices that offer an expert assessment on the offensive cyber capability of a state, but which do not offer supporting data (e.g. Belfer Center Cyber Power Index). Fourth, advanced Persistent Threats (APTs) that are not attributed to or were not found to have a formal relationship with their respective government. In these cases, the sources are labelled as Level 0 or n/a and still included in the database for context, but do not weigh in for the scoring in the declared and perceived capability ratings.

4.3. **Selection of nations**

The selection for nations is based on the criteria that they have a cybersecurity strategy and at least four datapoints. As of now, it covers 60 nations:

1. Albania
2. Argentina
3. Armenia
4. Australia
5. Austria
6. Azerbaijan
7. Bahrain
8. Belarus
9. Belgium
10. Brazil
11. Canada
12. China
13. Colombia
14. Croatia
15. Czech Republic
16. Democratic People's Republic of Korea
17. Denmark
18. Ecuador
19. Egypt
20. Estonia
21. Ethiopia
22. Finland
23. France
24. Germany
25. India
26. Indonesia
27. Iran
28. Israel
29. Italy
30. Japan
31. Kazakhstan
32. Lebanon
33. Malaysia
34. Mexico
35. Morocco
36. Netherlands
37. New Zealand
38. Nigeria
39. Norway
40. Pakistan
41. Poland
42. Qatar
43. Russia
44. Saudi Arabia
45. Singapore
46. South Korea
47. South Africa
48. Spain
49. Sweden
50. Switzerland
51. Syria
52. Thailand
53. Turkey
54. United Arab Emirates
55. United Kingdom
56. United States
57. Ukraine
58. Uzbekistan
59. Venezuela
60. Vietnam

5. Limitations

The Cyber Arms Watch is the first monitor of its kind that aims to measure to what extent nations are transparent about their offensive cyber capabilities. These capabilities are the most difficult to measure objectively. Amongst other things, this difficulty stems from the ambiguity, uncertainty, and duality inherent to cyberspace. This monitor aims to contribute to a first iteration of a Cyber Transparency Index, but recognizes several limitations that should be taken into account.

5.1. Definitions galore

The lack of clarity on exactly what capabilities exist in cyberspace means that it is very difficult to comprehensively describe the means (delivery systems or weapons) of such capabilities. There has been a debate about the term 'cyber weapons' ever since they have been used, without many conclusive outcomes on the usefulness of the term.[4] At best, a 'cyber weapon' is a weapon system of omni-use technologies that is extremely difficult for another state to verify due to a lack of transparency. As such, states are only left with the ability to presume – basically to guess – the overall capability of another state (albeit at widely varying degrees of detail) without, in most cases, being able to detail the exact order of battle, table of equipment, tactics, techniques and procedures (TTPs) or other basic information – unless the intelligence assessment is very complete. Instead, it makes more sense to approach cyber weapons as capabilities or operations.

This lack of agreed definitions originates from fundamental differences in how the West and the East understand cybersecurity. While the West has focused on the CIA triad, namely a fixation on the technical components of cyberspace or the status of data and systems, the East, particularly Russia and China, have looked beyond the technical components on the status of the data to include content. Their cyber capability mostly focuses on influence and psychological effects.

Nearly every country uses distinct cyber capability typologies that undergo constant change, which makes it very difficult to compare nations. This was recognized in the IISS Cyber Capabilities and National Power Assessment: "On offensive cyber, it has so far proved difficult even to find the language for a more informed national and international public debate, but such an effort remains essential if the risks are to be properly managed."[5] The issue is simply that they can cover the entire gamut of overt and covert action in cyberspace, meaning that virtually nothing is excludable. Traditionally, there is a very wide span of different understandings on how distinct elements of espionage, kinetic-equivalent, and psychological influence operations are categorised in and through cyberspace. There is also a practical differentiation between cyber effects that occur directly in the kinetic battlefield conducted at speed with and against military equipment (which usually are an approximation of Electronic Counter

4 Alexander Klimburg and Louk Faesen, "Balance of Power in Cyberspace," in Dennis Broeders and Bibi van den Berg (ed.), "*Governing Cyberspace: Behavior, Power, and Diplomacy*", (United Kingdom: 2020).

5 IISS Cyber Capabilities and National Power Index, p.5.

Measures), and strategic cyber, which largely uses conventional Internet technologies or even the Internet itself, and is often marked by a much slower operational tempo in multi-use computer networks (often associated with Advanced Persistent Threats).

The cyber capabilities discussed here cover that wide range of cyber operations, primarily focusing on cyber effect operations (from Level 3 onwards). It also includes cyber-enabled intelligence, surveillance and influence operations, as well as tactical or battlefield cyber capabilities that are sometimes called Cyber Electro-Magnetic Activities (CEMA). We recognise that offensive cyber is mostly used to deliver an effect (formerly known as Computer Network Attacks or CNA) rather than those intended to gather intelligence (formerly known as Computer Network Exploitation or CNE). Our declared capability rating follows this logic, in no small part because most nations disclose even less information about their covert intelligence capability and operations. For the perceived capability it was considered helpful to include CNE as the Level 1 label because very often it functions as a precursor for CNA and is indicative of an intrusive capability of states.

5.2. **Ambiguous language**

The lack of agreed definitions and the abundance of typologies for offensive cyber contributes to ambiguity. Unlike other military systems, offensive cyber capabilities are largely treated as dark secrets from the espionage world. Language used by governments to describe their declared cyber capability is often disguised and articulated in a defensive mould, using terms such as “active defence” or “(pro)actively responding.” Nor do all nations distinguish between offensive or defensive measures when referring to a cyber capability. Other nations refer to “informationised wars”, “cyber wars” or “realise cyber has become a weapon”. In other cases, states are ambiguous whether a capability is aspirational, under development, fully operational or already used.

Due to this embedded ambiguity, it is often difficult to ascertain whether there is indeed an offensive cyber capability lurking behind official government statements as well as the extent of this capability. Because of the nature of this *transparency* index, only direct references to an offensive capability or similar weigh in on the declared capability rating. Whenever a reference was considered too ambiguous, it was included but unlabelled. That way it offers additional context to the reader without affecting the transparency score. Otherwise, it would defeat the purpose of the index.

5.3. **Language limitations**

The high number of nations included in this index introduce language limitations in finding and understanding sources. This ranges from using the correct terminology in the local language for search terms to understanding the overarching cultural and military context of nations.

Research was first carried out in English using the generic term bucket of words to describe offensive cyber capabilities. This was followed by country-specific term buckets to refine the search terms in local languages, which was particularly useful for non-Anglo-Saxon countries. To this end, we combine neural machine translation services with native speaker experts. The translated term buckets allowed us to significantly expand the number of sources and

statements found on a nation's offensive cyber program. Those statements were then translated to English and captured in the database along with the original text. We recognize that some translations of key terms and sources may be linguistically inaccurate, in particular when solely relying on neural machine translation services. Likewise, the translated excerpts are not always entirely accurate, but should convey the key message clearly.

5.4. **Data availability and bias**

The purpose of this index is to bring greater transparency to the disclosure of offensive cyber capabilities. Hence, the underlying database is based on publicly available sources, which remains limited at best. There are many underlying reasons for this lack of data. First, is the very nature of cyber capabilities, being intelligence-driven, perishable and invisible, as well as ambiguous state-proxy relationships. Second, only a limited number of nations have a mature offensive cyber program. Most nations do not yet have such an offensive capability with effects that go beyond intelligence gathering, or have yet to operationalize it efficiently within their military, or face major technical, legal or institutional challenges in the process.

Third, the availability of information in the declared capability rating depends on nations willingness to disclose information about their offensive program. While there is improvement in this regard, as increasingly more nations openly disclose that they have offensive cyber capabilities, willingness remains limited, especially when it concerns disclosures that go beyond a mere acknowledgement of their capability. At the same time, some governments categorically reject they have an offensive capability or remain opaque about its existence, even when the perceived consensus believes otherwise. To this end, the limitation mentioned in the IISS Cyber Capabilities and National Power Index is a helpful reminder: "Offensive cyber and intelligence capabilities are, unsurprisingly, the most difficult to measure objectively. For example, an absence of evidence for their existence does not equate to evidence of their absence."[6]

Fourth, the perceived capability rating partly relies on publicly available sources that report on past cyber operations of states. Cyberattack operations will often, but not necessarily, be apparent to system operators, either immediately or eventually, since they affect or remove user functionality. But overall, the bulk of cyber operations occur covertly and will go unnoticed by third parties (or even the target). Again, just because they are not observed, it does not mean that they are not taking place. Publicly available data therefore only looks at the tip of the iceberg of past cyber operations.

A data bias is also observed because more "Western" actors and sources (media, government, industry, civil society) report on adversarial operations, resulting in a large dataset and higher scoring of the perceived capability rating (PCR) for nations such as China, Russia, Iran and North Korea. These nations have shared very little information about their offensive program and have been attributed, sanctioned, and indicted for offensive cyber operations more often by Western governments and cybersecurity companies, than the other way around. Nonetheless, the number of Chinese and Russian government and non-state entities that are attributing Western actors is slowly increasing.

6 IISS Cyber Capabilities and National Power Index, p.4.

Finally, the reader should be aware that the sources compiled aim to be as complete as possible but cannot possibly be exhaustive. The database will be updated periodically, and readers can contribute new sources. In the spirit of transparency, all underlying data that contributes to the score is available to the reader and each nation also receives a data availability indication for both ratings to improve awareness of the limitations of the underlying sources.

The data availability metric is added and iterated as both a data availability rank and a boxplot visualization showing the distribution of the data availability count across the sample. The data availability rank is a count of how many documents constitute the scores awarded for the DCR and PCR and is represented as a per country rank. It is important to note that many countries have the same count of documents. For example, both Brazil and Canada DCR values are underpinned by 16 documents. Where countries have equality in the count of documents, they are awarded the same rank. So, the lowest bound of the rankings are less than the sample size – DCR rank is capped at 10, whilst there are 61 countries, for this reason. The second representation of data availability takes the form of a box plot. It is included to demonstrate to the viewer the sense of the distribution of count data. Noticing the distribution for DCR, it is apparent that there is a fairly even spread of document counts across the sample, but that the United States is considered an outlier based on a significantly higher document count. So, it is clear to understand that the United States has a markedly higher disclosure of documents pertaining to its cyber capabilities compared to other countries.

5.5. **Unclear state-proxy relations**

The Cyber Arms Watch measures to what extent state actors are transparent about their capability. One of the most well-known disclaimers in offensive cyber is that governments often make use of proxies or non-state actors in order to retain plausible deniability. In cyber-space, the monopoly of violence by the state is challenged by the dominant role of non-state actors in various shapes and forms (attacker, victim, medium, or carrier of attacks), as well as their unclear relationships with governments. When Estonia, in 2007, was hit by what has sometimes been called the first strategic cyberattack in history, it marked a watershed moment in the use of state-sanctioned cyberattacks to advance foreign policy goals. It also introduced a model for conflict in cyberspace fought by proxy to retain some degree of plausible deniability.

The perceived capacity rating does not consider non-state actors unless their development and/or use of the cyber capabilities is directed or sponsored by a government. This means that government involvement (delegation) or support (orchestration) weigh in on the scoring of the perceived capability rating of states. Advanced persistent threats (APTs) that have not been attributed to a government actor are still included in the database because they provide context, but they remain unlabelled and therefore do not weigh in on the scoring.

The reader should bear in mind that proving a government relationship remains difficult. The actual affiliation of actors can be multiple all at once (government, proxy, and rogue actor). States are not monolithic entities, and many different departments can engage in cyber operations, often leading to a cacophony of action, not only from varying mandates within government but also due to the activities of proxies and other state-affiliated organisations. Non-state actors involved in cyber operations take on various forms that can have a formal, informal, or seemingly no relationship with a government. There have been numerous efforts

to structure these relationships. To make sense of these symbiotic and changing relationships, one can refer to various models describing the proxy-state relationships, such as the one theorised by Tim Maurer (See textbox below on Three State-Proxy relationships).. This includes *delegation, orchestration, or sanctioning*.[7] According to Maurer, the relationship between the government and the proxy, and the latter's use, depends on a range of factors, including the domestic landscape (public-private cooperation, crime levels, etc.); the government agencies' preexisting relations with proxies; and their definition of *cybersecurity* or *information security*, where China and Russia put more emphasis on the content of data as a potential threat to domestic stability. Ultimately, the reader should bear in mind that some governments deliberately maintain loose relationships with their proxies in order to retain plausible deniability.

Three State-Proxy relationships

Delegation presumes a state's effective control over the proxy to which it hands over certain cyber operations. It is mostly used to describe the US government's relation to cybersecurity and intelligence companies and contractors. Formalised in contracts, it is the most formally framed, meaning they are relatively constrained.[8] They provide a talent base for the intelligence and military agencies that are increasingly contracted in from industry (instead of tasks being outsourced to them). They also attribute adversarial transgressions as well as provide useful technical intelligence and evidence that can be used to inform attributions of the US or allies. While the blurring between both groups is predominantly a Russian characteristic (which maintains close and fluid relations with criminal enterprises), any country will have some degree of the so-called revolving door in which parts of its cybersecurity workforce oscillates between government agencies and non-criminal private entities. While 'active cyber defence' by the private sector is unlawful in most states, including the US, it may be reconsidered as a lawful tool.[9] Many policy and legal questions remain, such as determining the level of confidence needed for attributing an attack before taking proportional actions, as well as defining what the latter would look like.[10]

Orchestration means a state actively backing a non-state actor, often with financial or logistical means. The Iranian government, for example, has provided financial support to students for carrying out cyber operations against the US, while the non-state Syrian Electronic Army (SEA), often described as the Syrian government's loosely governed elite cyber militia, was behind hacks of Western media outlets, human rights organisations, communications platforms, and US military websites. Interestingly, after the SEA disappeared in 2016, it resurfaced a year later in a different form, moving its focus from covert intelligence operations to a public relations extension of the government that seeks to

7 Tim Maurer, *Cyber Mercenaries. The State, Hackers and Power* (Cambridge: Cambridge University Press, 2018).

8 Ibid.

9 In 2017, the Active Cyber Defense Certainty Act was introduced in the US House of Representatives but failed to gain traction. A similar bill now resurfaced in a bipartisan proposal. Tom Graves, "Active Cyber Defense Certainty Act," Pub. L. No. H.R. 3270 (2019); US Senate media, "117th United States Congress 1st Session".

10 Global Commission on the Stability of Cyberspace, "Additional Note to the Norm against Offensive Cyber Operations by Non-State Actors," (November 2018).

spread disinformation and shape media narratives.[11] Russia is described as a country that uses both orchestration and sanctioning in its relations to proxies.

Sanctioning implies passive support or inaction by turning a blind eye to the proxy. This is arguably the largest category. In contrast to the much tighter restrictions and direction that the Chinese government places on its non-governmental actors, Moscow often stops short of directing non-state actors and allows criminal groups to carve out their path as long as they generally work towards Putin's goals. [12] The partnership between Russian cybercriminals and the intelligence community is one of convenience – cybercriminals offer resources (in particular recruitment) and infrastructure that are also useful for government cyber operations as well as for politics.[13] After all, it offers the Russian government a degree of plausible deniability as it hides behind criminal actors.[14] An added advantage is that these criminals offer 'noise' under which the more skilled government hackers can move undetected. The defining factor of the Russian 'information counter-struggle' is that it is executed by a 'Whole of Nation' approach, much like the Soviet-era notion of 'total defence' which not only encompassed government entities but all national resources. This corresponds to the description by Russia expert Mark Galeotti of how the Russia carries out this approach by outsourcing to volunteers, organised-crime groups, businesses, government-organised non-governmental organisations, the media, and other actors in the deployment of various active measures.[15]

Finally, China is described as having a state-proxy relationship that moved from sanctioning to orchestration, and eventually delegation. The Chinese government's increasing control over proxy actors, exercised via traditional militia groups or patriotic hackers, coincided with an incremental hardening of Chinese Internet governance and control. IP theft campaigns were mainly carried out by non-state forces and were likely a useful way to keep these forces busy and their attention focused on outsiders rather than on domestic – in particular government – targets. Government actors were not only hiding in the noise created by the non-state actors (at least until the Xi-Obama agreement in 2015 condemning cyber-enabled economic espionage), but actively encouraging civilian attacks as well.[16] Clearly, Chinese authorities exercise some degree of control over at least some of the non-governmental hacking groups, albeit it is not always clear to what extent the activity was actually directed, rather than simply encouraged or tolerated. Similar to Moscow, Beijing brings outside hackers into the government fold and is known for its fusion between military and civilian entities.

---

11 It has been reported that "offensive cyber operations continue, but overall the SEA appears less technically sophisticated and more concerned with shaping the media narrative, disinformation and restraining the public's online behavior. The new SEA includes a media office and regional offices in various Syrian governorates." Abdulrahman Al-Masri and Anwar Abas, "The new face of the Syrian Electronic Army," Opencanada.org (May 17, 2018).

12 More specifically, a distinction is made between three types of associations between the intelligence services and criminal groups: direct links (e.g. the case of Dmitry Dokuchaev – a former cybercriminal who was recruited by the FSB), indirect affiliations (e.g. GameOver Zeus botnet) and tacit agreement (activity without a clear link but allowed by the Kremlin, which turns a blind eye to it). The report found that it is very unlikely that these associations and activities will come to an end, although they may adapt to provide greater plausible deniability through fewer overt and direct links between the spooks and criminals. Recorded Future Insikt Group, Cyber Threat Analysis Russia," (September 2019).

13 Klimburg, *The Darkening Web.*

14 Andrei Soldatov and Irina Borogan, "The Red Web: The struggle between Russia's digital dictators and the new online revolutionaries," *Journal of Strategic Security, 8*(4): 122 (2015).

15 Mark Galeotti, "Putin's hydra: Inside Russia's intelligence services", European Council on Foreign Relations, (May 11, 2016).

16 Klimburg, *The Darkening Web*, 288.

6. **Contrasting** the CAW with other Cyber Capability Indices

Following the example of the Freedom House Index, the Cyber Arms Watch was envisioned as an interactive map that functions as a transparency index for nations' offensive cyber capability. It may appear to be closely related to other indices, such as the Belfer Center's National Cyber Power Index (NCPI) and the IISS Cyber Capabilities and National Power Assessment. There are two main distinguishing features between these two indices and the Cyber Arms Watch.

First, both the IISS and Belfer Center's indices cover offensive capabilities as one of the many components in their analysis of a nation's cyber power. Their analysis is therefore much broader and also includes diplomatic and economic considerations and the other instruments of cyber power. The Cyber Arms Watch focuses only on offensive cyber capabilities.

Second, the other indices are expert assessments of the quality of a nation's offensive cyber programme by evaluating the quality of its military doctrine, the size of their commands, or by assessing whether they have been attributed to an attack in the Council of Foreign Relations Cyber Operations Tracker, amongst other indicators. While they try to parse and evaluate the instruments and components that contribute to the overall quality of a nation's offensive program, the Cyber Arms Watch focuses on assessing a nation's transparency of its offensive cyber capability by comparing its declared capability (DCR) with outside perceptions of that capability (PCR). They offer insight in how advanced a nation's cyber programme is, but the reader should bear in mind that the main purpose is to provide insight into transparency, not the quality of a nation's offensive cyber program. Our six-tiered labelling system can of course be expanded and refined in the future to allow for a more exhaustive and nuanced qualitative assessment of a nation's offensive program, by including annual budgets, manpower, tools, mandates, institutional maturity.

7. **Feedback** and Next Steps

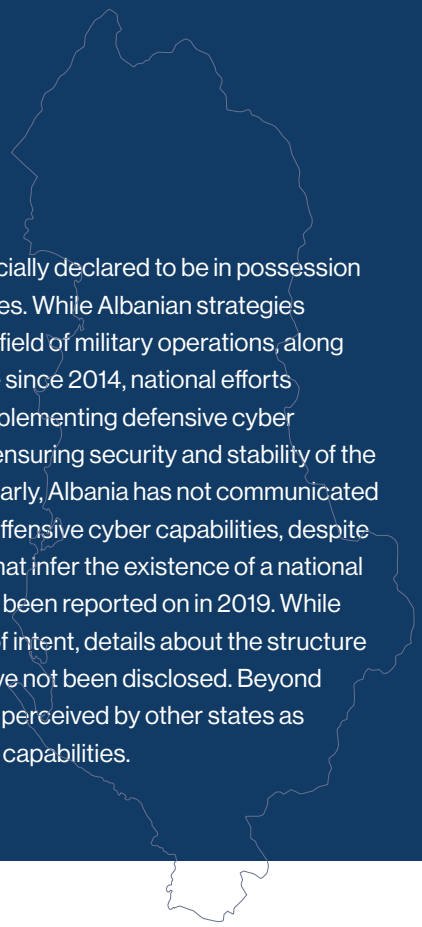
The Cyber Arms Watch is ever developing. We welcome your feedback, insights and input on the curation of the underlying data and labelling through the form at https://hcss.nl/cyber-arms-watch/.

With the support of the Municipality of The Hague, we were able to publish the first version of the Cyber Arms Watch monitor. With additional supporters, the second phase can be initiated: to support the establishment of a Cyber Transparency Board – a consortium of international experts that review and validate the labels of the Cyber Arms Watch, thereby contributing to much more robust methodology and objective result. The third phase would involve cluster analyses using the underlying database to draw attention to cluster relationships – for instance between groups of states within one rating group, or across both ratings. Where interesting clusters have been identified, secondary research will determine if these clusters have other commonalities – for instance in their Tactics Techniques and Procedures (TTPs), on an operational cyber level, but also in their engagement in diplomacy and international cybersecurity.

If you would like to be involved in or support the next steps of the Cyber Arms Watch, do not hesitate to contact info@hcss.nl.

8. Country Profiles

Albania



Cyber Transparency Score	**Transparent and Low Capability**
Declared Capability Rating	☐☐☐☐☐
Perceived Capability Rating	☐☐☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	48.05 (68th)
Internet Penetration (2020)	72%
Internet Freedom Score	n/a

Transparency Description

To date, Albania has not officially declared to be in possession of offensive cyber capabilities. While Albanian strategies recognise cyberspace as a field of military operations, along with air, sea, land and space since 2014, national efforts are currently focused on implementing defensive cyber capabilities with the aim of ensuring security and stability of the domestic cyberspace. Similarly, Albania has not communicated its aspirations to establish offensive cyber capabilities, despite nongovernmental reports that infer the existence of a national cyber command, which has been reported on in 2019. While this may be an early signal of intent, details about the structure and operative principles have not been disclosed. Beyond this, Albania is currently not perceived by other states as possessing offensive cyber capabilities.

Declared Capability Rating

Score ☐☐☐☐☐

No official Albanian indications of offensive cyber capabilities or aspirations were found. While there have been reports on the establishment of a military cyber command, the exact capacities of this unit have not been identified as of yet, but may be in future defence doctrines or strategies.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"A meeting was held on creating a military unit of Cyber Security," Albanian Armed Forces, November 15, 2019.	"In the premises of Ministry of Defence, a meeting was held to review the project of creating a military unit of cyber security for the AF... The Military Cyber Security Unit will be established in cooperation with our strategic partners as one of the priorities of the Defence Ministry and General Staff, as part of the modernization of defence capabilities and infrastructure in the Communications and Information Systems in the Armed Forces." Level 0
"Cross-Cutting Strategy "Digital Agenda of Albania 2015-2020", Albanian Ministry of Innovation and Public Administration.	No stated offensive cyber capability Level 0
"Defence Cyber Strategy," Albanian Ministry of Defence, November 6 2014	"The digital space of cyberspace is the fifth field of military operations in the world, along with air, sea, land and space." [Original: Fusha dixhitale e hapësirës kibernetike është fusha e pestë e operacioneve ushtarake në botë, së bashku me ajrin, detin, tokën dhe hapësirën.] Level 0

Perceived Capability Rating

Score ☐☐☐☐☐

No offensive cyber capabilities are perceived.

Data availability rating (1 being highest number of sources, 21 lowest): **20/21**

Document	Excerpt
"Cybersecurity in the Western Balkans: Policy gaps and cooperation opportunities," DiploFoundation, September 2016.	No mention of offensive capabilities. **Level 0**
"Report of Cybersecurity Maturity Level in Albania," Global Cyber Security Capacity Centre, 2018.	Supports the previous report: Albania is working on creating cyber defence, however none of its efforts are listed to transition into cyber offense. **Level 0**

Argentina

Cyber Transparency Score Transparent and Low Capability

Declared Capability Rating ■■□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber (2014):	Joint Cyber Defence Command (Comando Conjunto de Ciberdefensa)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	48.05 (71st)
Internet Penetration (2020)	86%
Internet Freedom Score	71/100 (Free)

Transparency Description

Argentina has disclosed its ambitions to develop offensive cyber capabilities. Following the announcement by the Ministry of Defence in 2020, Argentina established a Joint Cyber Defence Command (*Comando Conjunto de Ciberdefensa*) within the Joint Staff of the Armed Forces. The Unit is tasked with carrying out cyber defence operations. On several occasions, the Ministry of Defence has declared that it aims to develop capabilities to deal with conflict in cyberspace and to carry out actions to respond to potential hostile actors. However, to date, such developments remain aspirational as Argentina has not officially disclosed to having obtained or deployed offensive cyber capabilities. Outside perception supports the conclusion that Argentina is currently investing in upgrading its cyber arsenal. However, public reports hinting at Argentina's programme are quite dated and no relevant updates have been issued in this regard.

Declared Capability Rating

Score ■■□□□

Argentina has developed a Joint Cyber Defence Command responsible for carrying out operations in cyberspace. Among the operational priorities of the Centre is the development of deterrence and offensive response capabilities. However, to date, this development remains purely aspirational and Argentina has not officially disclosed to having obtained or integrated offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **2/10**

Document	Excerpt
"Comando Conjunto de Ciberdefensa del Estado Mayor Conjunto de las Fuerzas Armadas," Joint Chiefs of Staff of the Armed Forces, 2020.	Describes the actions and structure of the Cyber Defence Centre of the Armed Forces. Only defensive duties are mentioned. Level 0
"Argentina enfrenta los desafíos de la guerra cibernética," Juan Delgado, December 16, 2019.	"Faced with these challenges, Argentina seeks to strengthen its response capacities. In October 2019, the Ministry of Defence announced the creation of the National Cyber Defence Center, which will bring together the nation's defence platforms and systems such as the CCCD, as well as the creation of the Cyber Defence Advisory Committee to develop strategic military planning in cyberspace." Level 0

Document	Excerpt
"Resolución 1380/2019," Ministerio de Defensa, October 25 2019.	Resolution 1380/2019 brings into effect a cyber defence coordination body, the National Cyber Defence Centre: "The National Cyber Defence Centre is created within the SUBSECRETARIAT OF CYBER DEFENCE, where the INFORMATION EMERGENCY RESPONSE CENTRE OF THE MINISTRY OF DEFENCE (CSIRT of DEFENCE) will operate, the INTELLIGENT SECURITY OPERATIONS CENTRE (iSOC) of the JOINT COMMAND FOR CYBER DEFENCE of the JOINT STAFF OF THE ARMED FORCES, which centralises the operation of the remote SECURITY OPERATIONS CENTRES (iSOC) of each of the Armed Forces, and the CYBERNETIC ANALYSIS LABORATORY (CyberLab), among other platforms and systems, whose activities and implementation mechanisms will be defined by the SUBSECRETARY OF CYBER DEFENCE through the relevant acts." [Original: Créase el Centro Nacional de Ciberdefensa en el ámbito de la SUBSECRETARÍA DE CIBERDEFENSA, donde funcionarán el CENTRO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS DEL MINISTERIO DE DEFENSA (CSIRT de DEFENSA), el CENTRO INTELIGENTE DE OPERACIONES DE SEGURIDAD (iSOC) del COMANDO CONJUNTO DE CIBERDEFENSA del ESTADO MAYOR CONJUNTO DE LAS FUERZAS ARMADAS que centraliza la operación de los CENTROS DE OPERACIONES DE SEGURIDAD (iSOC) remotos de cada una de las Fuerzas Armadas y el LABORATORIO DE ANÁLISIS CIBERNÉTICO (CyberLab), entre otras plataformas y sistemas, cuyas actividades y mecanismos de implementación serán definidos por el SUBSECRETARIO DE CIBERDEFENSA a través de los actos pertinentes.] **Level 0**
"Resolución 1380/2019," Ministerio de Defensa, October 25 2019.	In this resolution, the Ministry of Defence states its aim of "developing capabilities to deal with conflict in cyberspace and execute actions to protect, monitor, analyse, detect and respond to potential adversaries or hostile agents that affect the integrity and availability of the Armed Forces' communication and information technology systems" [Original: desarrollar capacidades para enfrentar el conflicto en el ciberespacio y ejecutar acciones para proteger, monitorear, analizar, detectar y responder a potenciales adversarios o agentes hostiles que afecten a la integridad y disponibilidad de los sistemas de comunicación e informática de las Fuerzas Armadas]. It also states that the Subsecretary of Cyberdefence should "take preventive monitoring actions against potential adversaries or hostile agents acting in cyberspace that intend to affect the operational availability of the critical infrastructure of essential services" [Original: La Subsecretaria de Ciberdefensa debe realizar acciones preventivas de monitoreo contra potenciales adversarios o agentes hostiles que actuando en el ciberespacio, pretendan afectar la disponibilidad operativa de la infraestructura crítica de servicios esenciales]. **Level 2**
"Resolución 1380/2019 - Anexo 4", Ministerio de Defensa, October 24 2019.	Building on Resolution 1380's goal to "develop capabilities to deal with conflict in cyberspace," Annex 4 specifies the operational priorities of the Ministry of Defence in cyberspace, to be addressed in coordination with the different actors of the Defence System within the CyberLab of the National Cyber Defence Center among which it mentions "the development of deterrence and offensive response capabilities to threats of attacks that compromise freedom of action in cyberspace" (P.3) [Original: Desarrollar capacidad de disuasión y aptitudes ofensivas de respuesta ante amenazas de ataques que comprometan la libertad de acción en el ciberespacio] **Level 2**
"Argentina ya tiene listo su Centro Nacional de Ciberdefensa," Agustin Larre, May 12, 2019.	Covered the opening of a National Cyber Defence Centre, which "will serve to train military personnel so that they can protect, monitor, analyze, detect, and respond to such [cyber] activities." Clearly lists "respond" as one of the goals. **Level 0**
"Decreto 703/2018," Ministerio de Defensa, July 30 2018.	The decree states that "the National Defence requires adopting measures and actions aimed at safeguarding the cyber security of the critical infrastructures of the National Defence System and those designated for its preservation, regardless of the origin of the aggression." [Original: La Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión.] After mentioning that other countries have already developed "cutting-edge cyber capabilities to ensure the security of their critical or strategic IT infrastructures" [Original: capacidades cibernéticas de vanguardia, a fin de garantizar la seguridad de sus infraestructuras informáticas críticas o estratégicas], it states that Argentina must "adapt their military organizations to the emerging impact of these new [offensive cyber] risks. The cyber defence policy must be oriented to the gradual reduction of the vulnerabilities that emerge from the computerization of strategic assets of interest to the National Defence" [Original: La REPÚBLICA ARGENTINA debe adecuar sus organizaciones militares al impacto que emerge de estos nuevos riesgos. La política de ciberdefensa debe orientarse a la reducción gradual de las vulnerabilidades que emergen de la informatización de los activos estratégicos de interés para la Defensa Nacional.] **Level 0**

Perceived Capability Rating

Score 

Very few recent public reports have been published on Argentina's offensive cyber capabilities. The reports that state it is developing such capabilities date back to 2011 and 2013 and no further updates were found on the state of their capabilities.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"A System Dynamics Model of Cyber Conflict," Dana Polatin-Reuben; Richard Craig; and Theodoros Spyridopoulos, October 2013.	"In February 2010 Argentine hackers defaced the website of the Falkland Islands' weekly newspaper, Penguin News, with material supporting Argentina's claim of sovereignty over the Falklands. This attack was launched amidst diplomatic tensions between Argentina and the United Kingdom over proposed oil drilling in Falklands waters. While this cyberattack was small and not necessarily funded by the Argentinian government, it was clearly motivated by the sovereignty issues surrounding the Falkland Islands." (P. 4). **Level 0**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	Lists Argentina as one of 12 nations that intends to develop cyberwarfare organisations within the next year (report published in 2011). (P.4). It claims that "Argentine military officials have stated that information warfare capabilities should include both defensive measures to protect one's own networks and offensive measures to disrupt those of the enemy." (P. 5) Goes on to claim that "The Argentine Army's Communications and Computing Systems Command includes "Computer Science Troops" who implement a comprehensive doctrine that includes "cybernetic operations" for the cyberspace battlefield." (P. 5). **Level 2**
"Argentina, Brazil agree on cyber-defence alliance against US espionage," RT, September 13 2013.	One of the reported steps for cooperation between Brazil and Argentina, starting in 2014, is that Brazil would provide Argentinian officers with cyber warfare training. **Level 0**

Armenia

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	35.06 (90th)
Internet Penetration (2020)	77 %
Internet Freedom Score	71/100 (Free)

Transparency Description

A lack of transparency is observed for Armenia. On the one hand, no official indication of offensive cyber capabilities has ever been disclosed. The National Security Strategy, which is the sole official document released, prioritises the goal of enhancing cyber defence by boosting the Army's efficiency, protecting critical infrastructures and improving cybersecurity. However, on the other hand, Armenia is perceived as having either launched or obtained the ability to launch some forms of cyberattacks. In this regard, prior to 2020, sources reported on Armenia's alleged support to several APTs active against Azerbaijan, and even on a possible collaboration with Russia. After 2020, several news outlets detailed that the conflict with Azerbaijan had entered into new scenarios, with both States using DDoS attacks against each other, as well as undertaking disinformation campaigns through bots.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability. Armenia's latest security strategy contains a good deal of attention dedicated to cyber, however, no concrete mentions of offensive cyber capabilities are made.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Document	Excerpt
"National Security Strategy of the Republic of Armenia," Armenia, July 2020.	"In pursuit of our defence objectives, we shall continue to modernize our armed forces, develop command and control systems, improve military capabilities, raise the institutional efficiency of the armed forces, protect critical infrastructure, improve cybersecurity, and accelerate the progress of science and technology that contributes to the military industry. We shall also develop comprehensive mobilization capabilities." Level 0

Perceived Capability Rating

Score 

Perceived to have either launched or obtained the ability to launch some forms of cyber-attacks. Prior to 2020, Armenia's perceived interest in cyber operations was fairly limited (to supporting APTs). However, in 2020, several news outlets reported that the Armenia-Azerbaijan conflict had spread online, with both states using DDoS attacks and spreading cyber-enabled disinformation through bots.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"Armenia-Azerbaijan Clashes Spread Online," Manya Israyelyan, August 3 2020.	Despite the lack of much attention being paid to Armenian cyber capabilities, apparently, they were used in August 2020 against Azerbaijan, when Armenian-sponsored hackers launched a DDoS attacks against Azerbaijani websites and citizens in response to the former's DDoS attacks against Armenian websites as well as disinformation. **Level 3**
"Russian Loan Allows Armenia to Upgrade Military Capabilities," Eduard Abrahamyan, January 8 2020.	Russia gave Armenia a $100 Million USD loan to upgrade their military capabilities. Some have interpreted some of Armenia's plans with this money to develop "a so-called cyber-military-industrial complex, integrating the private IT sector with the MoD-regulated military industrial framework." **Level 2**
"Information Security or Cybersecurity? Armenia at a Juncture Again," Albert Nerzetyan, March 2018.	Implies that Armenia is not too invested in cyber operations and that Armenia's 2009 policy on cyber defence/security is simply a copy of the Russian version. **Level 0**
"Armenia at the Center of State-Sponsored Cyber Attacks," Samvel Martirosyan, January 19, 2018.	There are allegations that the Armenian state has been sponsoring several APT groups, or at least in collaboration with Russia. **Level 3**
"Armenia to Participate in Kazakhstan CSTO Drills," Joe Peerson, August 12 2014.	"Three thousand soldiers from six countries will take part in psychological and cyber warfare exercises when they meet for combat maneuvers in Kazakhstan on August 18 to 22, Aysor reports. The armed forces are gathering for the first time to participate in war games under the Collective Security Treaty Organisation (CSTO), which unites Rapid Reaction Force units from Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan." **Level 2**
'Patriotic hackers' in Armenia and Azerbaijan escalate crisis with cyber-attacks, Gohar Abrahamyan, September 7 2012.	This report claims that Armenian 'Patriot Hackers' have launching cyberattacks against Azerbaijan in this conflict. However, no clear link to the government was reported. **Level 0**

Australia

Cyber Transparency Score Transparent and High Capability

Declared Capability Rating ■■■■□

Perceived Capability Rating ■■■■□

Organization for Offensive Cyber (2018):	Information Warfare Division, Australian Signals Directorate
National Cyber Power Index (2020)	20.04 (10th)
National Cybersecurity Index (2022)	66.23 (37th)
Internet Penetration (2020)	90%
Internet Freedom Score	75/100 (Free)

Transparency Description

Australia disclosed that it has offensive cyber capabilities in several official documents and statements. In the latest Cybersecurity Strategy (2019), the government released information regarding the tasks of the Information Warfare Division (IWD), established in 2017 to synchronise efforts with the Joint Cyber Unit. Australia's declared capabilities comprise the ability to deploy offensive measures capable of disrupting, denying, or degrading hostile systems. The Cyber and Electronic Warfare Division of the Ministry of Defence further provides effective support in detecting threats and deploying electronic countermeasures. In 2020, the Deputy Chief Information Warfare even presented a highly conceptual framework for cyberspace operations which expressly referred to the deployment of offensive "cyber fires" capabilities. Most details about the organisational structure and specific capabilities are limited to tactical cyber and electromagnetic activities (CEMA), whereas information is fairly limited when it comes to the strategic cyber capabilities of the Australian Signals Directorate (ASD) and the Information Warfare Division. Furthermore, the 2020 military cyber doctrine remains classified. In light of the above, Australia is increasingly perceived as a cyber power equipped with significant offensive cyber capabilities. However, since reported cyber operations are mostly limited to countering lower-tiered non-state actors, Australia has also been regarded as a nation with higher intent than capability.

Declared Capability Rating

Score ■■■■□

Australia is transparent about its offensive cyber capability and its use. Most details abouts the organisational structure and specific capabilities are limited to tactical cyber and electromagnetic activities (CEMA), whereas those details are fairly limited when it comes to their strategic cyber capabilities by the ASD and the Information Warfare Division. The respective military cyber doctrine from 2020 remains classified.

Data availability rating (1 being highest number of sources, 10 lowest): **3/10**

Document	Excerpt
"State-Linked Cyber Actors Could Face Counter-Attack From Australia: Intelligence Boss," The Epoch Times, November 18, 2021	According to The Epoch, the director-general of the Australian Signals Directorate (ASD) Rachel Noble told Australian Associated Press that "the strength of Australia's offensive operations had grown to the point that the nation was now capable of shortening any war it got involved in."... "She said that while Australia would never seek out conflict, its intelligence capabilities allowed the ASD to "undertake offensive cyber operations as no one else can." Level 3

Document	Excerpt
"Information Warfare Division," (2), (3) Australian Dept. of Defence, July 1, 2020.	The Information Warfare Division (IWD) was formed in 2017 under Joint Capabilities Group within the Department of Defence to synchronise national efforts, with the Joint Cyber Unit as its main operational arm. This Unit operated alongside the Joint SIGINT Unit, alongside civilians teams of the ASD (intelligence service), under a new structure, namely the Defence Signals Intelligence and Cyber Command. In a presentation by the Deputy Chief Information Warfare, a high-level conceptual framework for cyberspace operations include offensive cyber capabilities, described as "cyber fires". A new ADF military doctrine for cyberspace operations was also issued in 2020 but remains classified. **Level 3,5**
"Cyber and Electronic Warfare Division," Australian Department of Defence, 2020.	"The division applies its capabilities to support situational awareness of the cyber and electromagnetic ... reliable and resilient cyber and EW systems ... and effective operations (including through computer network defence, and threat detection, warning and electronic countermeasures)." **Level 3**
"Australia's 2020 Cyber Security Strategy," Australian Government, 2019.	"At the other end are offensive measures to disrupt, deny or degrade the computers or computer networks of our adversaries. These tightly regulated tools belong exclusively to the Australian Government and are high cost and high risk." (P. 14) **Level 3**
"RAAF launches new cyber force," Bel Scott, November 1, 2019.	On October 31, Air Force introduced two new employment categories — cyber warfare officer (CWO) and cyber warfare analyst (CWA)." **Level 3**
"ASD Corporate Plan 2019-2020," Australian Signals Directorate, 2019.	The plan reiterates the principal cyber-related agency, the Australian Signals Directorate (ASD), commitment to the development and use of offensive cyber capabilities for national security and warfighting purposes. **Level 3**
'National Security Update on Counter Terrorism: Address to the House of Representatives, Parliament House, Canberra', 23 November 2016.	The Prime Minister acknowledges the use of offensive cyber capabilities against the Islamic State. **Level 3**
"Cyber and Electronic Warfare Division: Strategic Plan 2016-2021," Australian Dept. of Defence, 2016.	Official strategy plan of the cyber and electronic warfare division (CEWD) that focuses on cyber and electromagnetic activities (CEMA) in the battlefield, which include cyber and electronic attacks. It also features a detailed organisational chart of the CEWD. **Level 4**

Perceived Capability Rating

Score 

While outside reports on Australia's offensive programme are limited, it is perceived to have integrated offensive cyber capabilities into their military structure and use it (either literally or as a deterrent) to achieve strategic objectives. Over the past few years, Australia is increasingly recognised as an offensive cyber power, albeit in some cases described as a nation with higher intent than capability. Reported offensive operations are mainly limited at lower-tiered non-state actors, such as cybercriminals and ISIS.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Australia was ranked as #14 for their cyber offense capabilities. Overall, Australia finished as the #10 cyber power. This has caused some to be critical of Australian cyber actions. **Level n/a**
"Australia Spending Nearly $1 Billion on Cyberdefense as China Tensions Rise," Damien Cave, June 30 2020.	The article states that" The investment of 1.35 billion Australian dollars ($930 million) over the next decade is the largest the nation has ever made in cyberweapons and defences." This new investment comes in response to increasing Chinese cyberattacks. **Level 2**
"Australian government says it is hacking criminals who are exploiting the pandemic," Sean Lyngaas, April 7 2020.	"The ASD, the country's lead agency for hacking operations, has "already successfully disrupted activities from foreign criminals by disabling their infrastructure and blocking their access to stolen information," **Level 3**
"Australia's Offensive Cyber Capability," Fergus Hanson and Tom Uren, 2018.	Outlines what it believes to be the current structure of Australian offensive cyber operations and current/past operations: "Australia has declared that it will use its offensive cyber capabilities to deter and respond to serious cyber incidents against Australian networks; to support military operations, including coalition operations against Daesh in Iraq and Syria; and to counter offshore cybercriminals." **Level 4**
"Snowden documents reveal Australia tapped Indonesian president's Nokia: Report," Chriss Duckett, November 18 2013.	Snowden revealed some documents showing that Australia had been using cyber power to spy on their neighbors (especially Indonesia). The Prime Minister dismissed these claims: "Australian Prime Minister Tony Abbott said that "all governments gather information" and that such revelations were "hardly a shock". **Level 1**
"Cyber Warfare: Critical Perspectives," Paul Ducheine, Frans Osinga, Joseph Soeters (eds.), 2012.	This Dutch review of military studies in 2012 identifies Australia as developing or possessing significant cyber powers. However, it states that at the time, "it remain[ed] unclear whether an offensive or even a counterattacking defence capability is envisioned by the Australians." (P. 42). **Level 2**

Austria

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber:	Direktion IKT & Cyber (ICT & Cyber Directorate)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	68.83 (31st)
Internet Penetration (2020)	88%
Internet Freedom Score	n/a

Transparency Description

Since 2016, Austria has acknowledged the importance of pairing defensive and offensive cyber capabilities in cyberspace. The 2017 Military Strategy expressly requires Austrian cyber forces to master the full spectrum of combat in computer networks, including defence, exploitation, and attack. Official documents further detail that Austria is significantly investing on enhancing defensive cyber capabilities, also by developing and using offensive components, but no information regarding the current progress has been released yet. Very few outside sources report on Austria's offensive capabilities. One report maintained that military cyber forces have been established already, but no official acknowledgment has been issued in this regard.

Declared Capability Rating

Score ■■■□□

Sanctioned media reporting on offensive cyber details and/or operations by an official (capabilities likely to exist but unconfirmed by official resources, the extent of which being unknown). Austria mentions that it is stocking up on cyber defence capabilities including offensive components to deter cyberattacks. Recently, it has disclosed the structure of its Cyber Forces, which include a Unit (the Cyber Force) tasked with carrying out offensive cyber operations to counter cyber attacks. No further details nor military cyber doctrines have been released so far.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"Cyber runs the system", Austrian Armed Forces, 2019	The website of the Armed Forces details the structure of the Austrian Cyber Forces, which are fully integrated within the military and consist of three units: (i) the Cyber Force; (ii) the ICT Force; and (iii) the Electronic Warfare Force. The Cyber Force is tasked with countering cyberattacks and masters the full spectrum of combat in computer networks (defence, exploitation, and attack). The ICT Force plans, builds, and operates the ICT systems of the Armed Forces and provides the necessary technology for the troops in every circumstance. Finally, the Electronic Warfare Force is tasked with collecting, identifying, evaluating, and preparing information in the electromagnetic spectrum. [Original: "Die Cyberkräfte bestehen aus der Cyber-Truppe, der IKT-Truppe und der EloKa-Truppe für elektronische Kampfführung... Die Cyber-Truppe begegnet Angriffen im Cyberraum. Das bedeutet: Sie beherrscht das volle Spektrum des Kampfes in Computernetzwerken (Verteidigung, Ausnützung, Angriff). Die IKT-Truppe plant, errichtet und betreibt die IKT-Systeme des Bundesheeres. Sie stellt im Alltag sowie bei Übungen und Einsätzen im In- und Ausland die erforderliche Informations- und Kommunikationstechnologie für die Truppe bereit. Die EloKa-Truppe hat speziell für das elektromagnetische Spektrum die Aufgabe, Informationen unter Nutzung technischer Mittel zu erfassen, zu identifizieren, auszuwerten und für die jeweilige Führungsebene aufzubereiten.] Level 3

Document	Excerpt
"Militarstrategisches Konzept 2017," Osterreichisches Bundesheer, 2017.	"The cyber forces must master the full spectrum of combat in computer networks (defence, exploitation and attack)." (P. 14) [Original: Die Cyber-Kräfte müssen das volle Spektrum des Kampfes in Computernetzwerken beherrschen (Verteidigung, Ausnützung und Angriff)] Level 1
"Bundesheer setzt auf offensive Cyberwaffen," Markus Sulzbacher, October 18, 2016.	"Striedinger and his team are currently building a cyber defence center to combat such attacks effectively. This should also have offensive weapons for warfare online. [...] Every defence needs an offensive component. This is the case in the real world and it is the same in the cyber world," says Striedinger. How the army comes to such digital weapons is still being discussed internally. "It's about the army having the capabilities that other states and terrorists already have." [Original: "Um derartige Angriffe wirksam zu bekämpfen, bauen Striedinger und sein Team gerade ein Cyber-Defense-Center auf. Dieses soll auch über offensive Waffen zur Kriegsführung im Netz verfügen. [...] Jede Verteidigung braucht eine offensive Komponente. Das ist in der realen Welt so und das ist auch in der Cyberwelt so", sagt Striedinger. Wie das Heer zu solchen digitalen Waffen kommt, wird derzeit noch intern beredet. "Es geht darum, dass das Heer solche Fähigkeiten hat, wie sie andere Staaten und Terroristen bereits haben."] Level 1
Bundesheer, Offensiv in der Cyberverteidigung (FOKUS Magazine), March 2016.	Describes under what conditions offensive cyber measures may be taken, such as in the event of a serious cyberattack that has serious implications for the sovereignty of the state or attacks against military and critical infrastructure. Level 2

Perceived Capability Rating

Score ■■□□□

Perceived to be working on obtaining offensive cyber capabilities. Very few reports were found that mention anything about Austria's progress to this end.

Data availability rating (1 being highest number of sources, 21 lowest): **20/21**

Document	Excerpt
National Cyberdefense Policy Snapshots, Sean Cordey and Robert S. Dewar, ed., September 2019.	This report mentions that "military cyber forces with offensive capacities have been established" (P. 8) in Austria, but again does not specify any details. Level 2
"Democratic Governance Challenges of Cyber Security," Benjamin Buckland, Fred Schreier, Theodore Winkler, 2015.	This report describes the existing structure for the governance of cybersecurity in Austria as: "Department II of the Ministry of Defence is responsible for all aspects of information warfare and fulfils its duties in close cooperation with the two intelligence services." (P. 33). No mention of the capacity or examples are given. Level 0

Azerbaijan

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	37.66 (85th)
Internet Penetration (2020)	85 %
Internet Freedom Score	35/100 (Not free)

Transparency Description

A lack of transparency is observed for Azerbaijan. While no official information has ever been disclosed with regard to either the possession of or aspiration to develop offensive cyber capabilities, Azerbaijan is perceived as having either launched or obtained the ability to launch some forms of cyberattacks. In particular, several sources reported on the use of DDoS attacks by Azerbaijan in the context of the conflict with Armenia. Other than that, Azerbaijan is mostly perceived as having acquired several surveillance tools for domestic surveillance purposes.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■■☐☐

Perceived to have either launched or obtained the ability to launch some forms of cyberattacks. There are few sources detailing the existence of Azerbaijani offensive cyber capabilities, which are mostly linked to domestic surveillance tools or DDoS attacks as part of Azerbaijan's conflict with Armenia.

Data availability rating (1 being highest number of sources, 21 lowest): **15/21**

Document	Excerpt
"Private Israeli spyware used to hack cellphones of journalists, activists worldwide," Dana Priest, Craig Timberg and Souad Mekhennet, July 18 2021.	Azerbaijan has acquired surveillance and intelligence tools on several occasions the Israeli company NSO. Level 1
"Armenia-Azerbaijan Clashes Spread Online," Manya Israyelyan, August 3 2020.	Reports that Azerbaijan committed several cyberattacks (DDoS and bots spreading disinformation) against Armenia when tensions flared in summer 2020. Armenia also responded with DDoS attacks. Level 3
"Deep Packet Inspection and Internet censorship in Azerbaijan," VitualRoad/Qurium, April 1 2017.	This internet freedom organisation noted in 2017 that the Azerbaijani government was blocking various websites. Level 1

Document	Excerpt
"News Media Websites Attacked From Governmental Infrastructure in Azerbaijan," Qurium, March 10 2017.	The report informs of numerous DDoS attacks against independent media in Azerbaijan. It also reports on instances of "intrusion attempts, spear-phishing campaigns and electronic media monitoring," all of them attributed to the government of Azerbaijan. According to Qurium, the government uses "AutoItSpy", a home-grown surveillance tool to exfiltrate information from Azerbaijani human right activists. **Level 3**
"Azerbaijan: Activists targeted by 'government-sponsored' cyber attack," Amnesty International, March 10 2017. (1) "False Friends: How Fake Accounts and Crude Malware Targeted Dissidents in Azerbaijan," Amnesty Global Insights, March 10 2017. (2)	Amnesty international claimed here that "Our research reveals that a targeted and coordinated cyber campaign is being waged against critical voices in Azerbaijan, many of whom are long-time victims of government repression." The main tools used were malware, with strategies like spearfishing. The Azerbaijan government denied these accusations. **Level 1**
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	Azerbaijan has acquired surveillance and intelligence tools on several occasions from the Italian firm Hacking Team. **Level 1**

Bahrain

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■☐☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	25.97 (106th)
Internet Penetration (2020)	100%
Internet Freedom Score	30/100 (Not free)

Transparency Description

Bahrain has not disclosed it has offensive cyber capabilities nor any aspirations. During the 2019 defence conference (BIDEC), Bahrain declared that its main goal is to enhance defensive cyber capabilities in order to be able to respond to the increasing offensive capabilities developed by Iran. From the outside, Bahrain's offensive cyber capabilities are perceived as fairly limited to domestic surveillance tools and spywares, which Bahrain reportedly acquires from foreign vendors such as FinFisher Gmbh's and NSO.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Document	Excerpt
"BIDEC 2019: A Window into Bahraini Perspectives on Defense and Security," Robbin Laird, November 2, 2019.	Based on second-hand report of a Bahraini perspective on the future of defence, there was a stated aspiration to increase their cyber defence (without explicitly mentioning offensive capabilities), driven largely by increasing Iranian cyber capabilities. Level 0

Perceived Capability Rating

Score ■☐☐☐☐

Bahrain's offensive cyber capability is perceived to be limited to spyware tools it acquired from foreign vendors.

Data availability rating (1 being highest number of sources, 21 lowest): **17/21**

Document	Excerpt
"Private Israeli spyware used to hack cellphones of journalists, activists worldwide," Dana Priest, Craig Timberg and Souad Mekhennet, July 18 2021.	The report states that Bahrain has acquired surveillance and intelligence tools on several occasions from Israeli company NSO. Level 1

Document	Excerpt
"German-made FinSpy spyware found in Egypt, and Mac and Linux versions revealed," Amnesty International, September 25 2020.	The report identifies Bahrain as one of the countries to have bought FinFisher Gmbh's spyware tools. **Level 1**
"Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, September 18 2018.	The report accuses Bahrain of making extensive use of spyware (specifically Pegasus from the NSO group) to target journalists and other citizens. **Level 1**
"Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East," Kristina Kausch, November 24 2017.	The article mentions, in the cyber-offence context, that "Bahrain, on the front line as a small Shia majority state, has recently adopted a notably friendly public discourse on Israel." (P. 8). **Level 0**
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	Emails and financial records uncovered that Bahrain government agencies have bought Hacking Team spyware. **Level 1**

Belarus

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	53.25 (60th)
Internet Penetration (2020)	85%
Internet Freedom Score	31/100 (Not free)

Transparency Description

A lack of transparency is observed for Belarus. No reference to offensive cyber capabilities can be identified in official documents. At the same time, Belarus is perceived by other states as having either launched or obtained the ability to launch some forms of cyberattack. Belarus' capabilities are currently perceived as being largely focused on domestic surveillance aimed to crack down political dissent and opposition. Belarus is also suspected of having engaged in several cyber operations and cyber-enabled influence operations by sponsoring hacker groups, such as UNC1151.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of a declared offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **9/10**

Document	Excerpt
"Doctrine of Information Security of the Republic of Belarus," Belarus Ministry of Foreign Affairs, March 18 2019.	Belarus refers to cyberwarfare as 'information confrontation'. The 2016 Military Doctrine – updated from the 2002 version – does not appear to contain any mention of Belarus' supposed aspiration for cyber capabilities in 2002. **Level 0**
2016 Belarus Military Doctrine (Primary source not available online; secondary source below.) "Belarus's New Military Doctrine: What's the Message?," Belarus Digest, September 1 2016.	No offensive cyber capability in the updated 2016 military doctrine. **Level 0**

Perceived Capability Rating

Score ■■■□□

Perceived to have either launched or obtained the ability to launch some forms of cyberattacks. Belarus' capability is mostly limited to domestic surveillance and Internet shutdowns to crack down political dissent and opposition. Hacking group UNC1151, which is believed to be state-sponsored and allegedly has ties to Russia, is one of the most prominent examples in which Belarus has engaged in cyber-enabled influence operations abroad. It should be noted that Belarus has a mandatory System of Operative Investigative Measures (SORM) that requires all Internet Service Providers and telecom agencies to install equipment that allows the intelligence services to directly monitor all domestic Internet traffic without any notification to the providers or the users. At the same time, the government has also acquired surveillance tools from foreign vendors.

Data availability rating (1 being highest number of sources, 21 lowest): **13/21**

Document	Excerpt
"EXCLUSIVE Ukraine suspects group linked to Belarus intelligence over cyberattack," Pavel Polityuk, January 16 2022.	UNC1151 is suspected to be behind the defacement of Ukrainian government websites in January 2022, following increased border tensions and Russian military buildup along the border with the Ukraine. The Ukrainian government links the operation to the Belarusian group, which allegedly used malware similar to that used by a group tied to Russian intelligence. **Level 3**
"Taming the Bear: Russia's Huge Exercises Test NATO Resolve," CEPA, 1st September 2021	Joint Belarus-Russia testing of cyber capabilities is mentioned in the context of the Zapad exercise **Level 2**
"Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity," Mandiant Threat Intelligence, April 28 2021	Since releasing the previous public report on UNC1151, Mandiant tracked new incidents extending back years before the campaign was uncovered in 2020. A new report provides an update on Ghostwriter, highlighting two significant developments. First, an expansion of narratives, targeting, and TTPs associated with Ghostwriter activity (e.g. to create domestic political disruption in Poland rather than foment distrust of NATO). They have not relied on the dissemination vectors typically observed with previous Ghostwriter activity, such as website compromises, spoofed emails, or posts from inauthentic personas. Second, it was able to attribute with high-level confidence that UNC1151 conducts at least some components of Ghostwriter influence activity. **Level 3**
"Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity," Mandiant Threat Intelligence, April 28 2021.	The suspected state-sponsored Belarusian hacker group UNC1151 has repeatedly been associated with several cyber operations and cyber-enabled influence operations against Eastern European NATO members. The main aim of the Ghostwriter campaign was to steal information and fuel discord with narratives critical of NATO's presence in Eastern Europe. EU member states have previously suspected Russia's involvement in Ghostwriter, but this has not yet been formally confirmed by Mandiant (albeit also not ruled out). **Level 3**
Israeli phone hacking firm stops sales to Belarus and Russia, Tanya Lokot, April 5 2021	Cellebrite, an Israeli digital intelligence company known for making software tools used to extract data from smartphones, has announced it will halt sales to Russian and Belarus state and law enforcement. **Level 1**

Document	Excerpt
"Belarus Has Shut Down the Internet Amid a Controversial Election," Lily Hay Newman, Wired August 10 2020.	Dozens of reports confirm that Belarus continues to use cyber operations and internet shutdowns domestically. The most recent, and most prominent, was when in summer 2020 the Belarussian government shut down the internet in the nation following the controversial reelection of their President Lukashenko. The Belarussian government blamed the shut down on attacks coming from abroad, but this was contested by human rights organisations. **Level 1**
"Urgent appeal concerning Internet service disruptions in Belarus in the context of the presidential elections of 9 August 2020", 50 Human Rights Organizations, 10 August 2020.	Over 50 human rights organisations submitted a letter to the UN condemning the Belarussian government for its Internet shutdown in the context of the presidential elections of 9 August 2020. This is reinforced by US Secretary of State Mike Pompeo: "We strongly condemn ongoing violence against protesters and the detention of opposition supporters, as well as the use of internet shutdowns to hinder the ability of the Belarusian people to share information about the election and the demonstrations." **Level 1**
"Belarus: Submission to the United Nations Human Rights Committee. 124th Session, 8 October to 2 November 2018," Article 17, Amnesty International, Submission to the United Nations Human Rights Committee 124th Session, 8 October to 2 November 2018.	Belarus, like Russia, has a mandatory System of Operative Investigative Measures (SORM) that requires all Internet Service Providers and telecom agencies to install equipment that allows the intelligence services to directly monitor all domestic Internet traffic without any notification to the providers or the users. The authorities used it to monitor and interfere in political and human rights activities. While this does not qualify as an offensive cyber operation, it may lead to a lower need to acquire offensive or surveillance tools for domestic purposes. **Level 0**
"Armenia to Participate in Kazakhstan CSTO Drills," Joe Peerson, August 12 2014.	"Three thousand soldiers from six countries will take part in psychological and cyber warfare exercises when they meet for combat maneuvers in Kazakhstan on August 18 to 22, Aysor reports. The armed forces are gathering for the first time to participate in war games under the Collective Security Treaty Organization (CSTO), which unites Rapid Reaction Force units from Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan." **Level 2**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	This report explains about how, in wartime, Belarus has an "offensive repulsion" (P. 7) capability, explaining "they are trained in informational confrontation and counteraction against enemy forces." (P. 7). **Level 0**
"Strategic Cyber Security," Kenneth Geers, June 2011.	This publication has two sections that detail the use of government surveillance against its own citizens from 2001 onwards, when it used the state-owned telecommunications company Beltelecom to block opposition websites on the day of their national elections. The government officially claimed it was either a result of too many website visits at once or had no comment (P. 74-75). The government continued such tactics in subsequent elections, using DDoS to take down websites. (P. 75-76). **Level 3**

Belgium

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber (2021):	Cyber Directorate (MoD); ADIV (intelligence service)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	93.51 (3rd)
Internet Penetration (2020)	92%
Internet Freedom Score	n/a

Transparency Description

Belgium has officially disclosed its plans to develop offensive cyber capabilities and to fully integrate them within the military. The 2021-2025 Cybersecurity Strategy expressly mentioned that the Ministry of Defence is developing the capabilities to carry out counterattacks, as well as intrusive and offensive operations. Furthermore, the Belgian Intelligence services revealed that the Defence has developed a cyber capability to defend military systems and, if need be, to carry out offensive operations to support the military. However, to date, Belgian offensive capabilities remain largely aspirational. The tasks of the Military Cyber Directorate, established in 2021, are focused on enhancing defensive measures and no details regarding the Command structure, missions, conditions of employment, and overall principles for conducting offensive operations have been published. Belgium's perceived capabilities largely coincide with what the government has disclosed so far, but no offensive operations has ever been attributed to the government.

Declared Capability Rating

Score

Belgium seems to be developing or has already developed offensive cyber capabilities as part of its response mechanism. No further details about the command structures, missions, conditions of employment and overall principles are disclosed, nor has it published a dedicated military cyber strategy or doctrine.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
Website of ADIV/SGRS, Last accessed February 2022	According to the website of the Belgian intelligence service, ADIV/SGRS, the Defence forces have developed a cyber capability to defend military systems and, if need be, to offensively support military operations. This capacity is realised in the Directorate Cyber of the ADIV, which includes experts in offensive cyber operations. [Original: "Als antwoord op deze nieuwe dreiging, heeft Defensie een cybercapaciteit ontwikkeld die de opdracht heeft om de militaire systemen te verdedigen en desnoods op offensieve wijze militaire operaties te ondersteunen tegen de dreiging komende van het virtuele slagveld. Deze cybercapaciteit is gecentraliseerd in de directie Cyber van de ADIV. Experten van alle disciplines in het domein van Cyber Security zijn in de directie aanwezig maar ook, en dit is uniek in België, experten in offensieve cyber operaties." Level 3

Document	Excerpt
Website of ADIV/SGRS, Last accessed February 2022	According to the website of the Belgian intelligence service, ADIV/SGRS, the Defence forces have developed a cyber capability to defend military systems and, if need be, to offensively support military operations. This capacity is realised in the Directorate Cyber of the ADIV, which includes experts in offensive cyber operations. [Original: "Als antwoord op deze nieuwe dreiging, heeft Defensie een cybercapaciteit ontwikkeld die de opdracht heeft om de militaire systemen te verdedigen en desnoods op offensieve wijze militaire operaties te ondersteunen tegen de dreiging komende van het virtuele slagveld. Deze cybercapaciteit is gecentraliseerd in de directie Cyber van de ADIV. Experten van alle disciplines in het domein van Cyber Security zijn in de directie aanwezig maar ook, en dit is uniek in België, experten in offensieve cyber operaties." **Level 3**
"The Belgian Military Cyber Directorate," Belgian Defence, 2021.	"What is the cyber mission? The Belgian military Cyber Directorate ensures freedom of action in and through cyberspace by: (1) Guaranteeing the integrity, availability, and confidentiality of military networks and weapon systems. (2) Providing early warning and rapid reaction through advanced detection, monitoring and incident handling. (3) Collecting cyber threat intelligence on adversaries and vulnerabilities.(4) Delivering cyber effects for integration in intelligence and military operations. (5) Offering a continuous and challenging cyber education and training plan to acquire and sustain highest level cyber expertise." **Level 0**
"Cybersecurity Strategie Belgie 2021-2025," Centre for Cyber Security Belgium, May 2021.	Belgium's national cybersecurity strategy for 2021-2025 mentions that the Ministry of Defence (MoD) is developing a cyber strategy. It includes the capability to carry out counterattacks: "During national crises, the MoD needs to be able to carry out intrusive and offensive capabilities, allowing it to respond with its own cyberattack to neutralise the initial attack and to identify the perpetrators." [Original: "Tijdens nationale crisissituaties haar [Defensie] intrusieve en offensieve capaciteiten in te zetten om met een eigen cyberaanval te reageren om de aanval te neutraliseren en er de daders van te identificeren." **Level 2**
"Stafchef leger slaapt niet goed", De Tijd, 27 November 2020	In this article, the Chief of Defence, Michel Hofman, says that it is not only necessary to defend own networks, but "we have to be able to execute offensive operations. We have to be able to carry out counter-attacks against servers if we are being attacked from Russia or Iran." **Level 2**
"Cyber Security Strategy," Belgium, 2012.	No offensive capability or aspirations mentioned. **Level 0**

Perceived Capability Rating

Score ■■□□□

Perceived to be working on obtaining offensive cyber capabilities with most reports referring to governments statements. No past operations or campaigns were found.

Data availability rating (1 being highest number of sources, 21 lowest): **17/21**

Document	Excerpt
Het Belgische leger, waar hackers straks dingen mogen doen die ze nergens anders kunnen en durven, Nieuwsblad, January 31 2022.	In this Belgian newspaper article, it is reported that the Belgian national mandate allows for offensive cyber operations, and that a senior military official stated that cyber is an indispensable weapon within the modern armed forces. **Level 2**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	"Belgium plans to establish military cyber component in 2019." (P. 187). **Level 2**
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	When talking about offensive cyber power, the author notes that "We can expect several other newcomers in the near future. For example, according to the Belgian media, "the Belgian military forces are to get a new [cyber] component as from 2019"," (P. 10). **Level 2**
"Strengthening the EU's Cyber Defence Capabilities," Jaap de Hoop Scheffer, November 2018.	Reports that Belgium is an observer to the PESCO framework, an initiative that typically puts forth cyber defence projects which "explicitly illustrate a persistent demand for tactical and operational solutions to cybersecurity challenges." (P. 35). **Level 0**
"Belgium," UNIDIR Cyber Policy Portal, November 2018.	Lists that "Belgium will further develop its own cyber capability, consisting of a defensive, offensive and intelligence pillar." [...] "The offensive cyber capability in support of the expeditionary operations will be essentially based on a reach-back capability, physically located in our own country." **Level 2**

Brazil

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■■■■

Perceived Capability Rating ■■■□□

Organization for Offensive Cyber (2015): The Centre for Cyber Defence (Centro de Defesa Cibernética)

National Cyber Power Index (2020): Ranked as 30th (last) among all countries considered

National Cybersecurity Index (2022)	46.75 (75th)
Internet Penetration (2019)	81 %
Internet Freedom Score	64/100 (Partly free)

Transparency Description

Brazil scores well in terms of overall transparency. In fact, its declared capability is estimated to be much higher than its perceived capability. The government has released a significant number of detailed strategies and doctrine detailing its offensive cyber capabilities. In 2017, the Army published a military manual, detailing command structures, order of battle, the different types and forms of cyberattacks, and their integration in land operations. The manual builds up on the 2014 military cyber doctrine, which expressly includes offensive cyber capabilities and details missions, conditions for employment, overall operative principles, as well as TTPs. Brazil is also perceived to invest a considerable amount of resources to develop and deploy cyber capabilities. However, no offensive operation has ever been publicly attributed to Brazil.

Declared Capability Rating

Score ■■■■■

Brazil boasts a series of detailed and publicly-available cyber warfare strategies and doctrines from 2014 onwards that indicate a high degree transparency in the declared offensive cyber capabilities. This includes a defence cyber strategy and doctrine where offensive cyber capabilities are detailed, including available definitions of different types of cyber effects, detailed order of battle, as well as TTPs. It also is indicative of its integration within its overall concept of operations, Brazilian thinking on cyber, as well as their operational set-up and capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **7/10**

Document	Excerpt
"Comando Naval de Operações Especiais conduz exercício de Guerra Cibernética," Marinha do Brasil, September 22, 2020.	The document details a Brazilian cyber exercise to assess the effectiveness of the Navy's organisational structures and doctrinal instruments to carry out and counter limited cyberattacks, such as those perpetrated by hacktivist groups and cybercriminals without state support. Level 2
"Guerra Cibernetica," Brazilian Ministry of Defence, 2017.	The Brazilian Army published its campaign manual for cyberwar, detailing command structure, its order of battle, the different types and forms of cyberattacks, and their integration in land operations. Level 5

Document	Excerpt
"Comparative analysis of the structuring of the cyber industry national according to international cyber network doctrines," Electronic Warfare Instruction Centre, 2017.	The Brazilian Electronic Warfare Instruction Centre conducted a comparative analysis of the cyber doctrines of various European countries (including Estonia, France, UK, Netherlands and Spain), which also mentions Brazilian offensive cyber capabilities. **Level 3**
"Doutrina Militar de Defesa Cibernética", Brazilian Ministry of Defence, 2014	Brazil published its Military Doctrine for Cyber Defence in 2014, with details about its missions, conditions for employment and overall principles of operation. It also includes offensive cyber capabilities: "Cyber Defence – a set of offensive, defensive and exploratory actions carried out in the Cyber Space, in the context of a national level strategic planning, coordinated and integrated by the Ministry of Defence, with the purpose of protecting information systems of interest to National Defence, obtain data for the production of Intelligence knowledge and compromise the information systems of the opponent. They are possibilities of the Cyber Defence: a) to act in the Cyberspace, by means of offensive, defensive and exploratory actions." (P. 21) [Original: "Defesa Cibernética – conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no ontext de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente." (P. 18)"Possibilidades da Defesa Cibernética 2.5.1 São possibilidades da Defesa Cibernética: a) atuar no Espaço Cibernético, por meio de ações ofensivas, defensivas e exploratórias"] **Level 4**

Perceived Capability Rating

Score ■■■□□

There are quite a few sources detailing that Brazil military branch has an emphasis on different cyber warfare capabilities. It is further mentioned that Brazil has been involved in different cyber defence workshops and in collaborations with other cyber powers.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Brazil is placed last out of all countries in the report in terms of offensive cyber power. **Level 0**
"Brazil-Russia Military-Technical Cooperation," Military Review, Nov-Dec 2018.	Notes that Russia and Brazil often closely collaborate in the cyber area as well. **Level 2**
"New players join race for offensive cyber abilities," Oxford Analytica, August 20 2018.	Noted that while Brazilian cyber defence abilities have been demonstrated well, not much is known on Brazil's offensive capabilities. The report speculates that one significant, unattributed APT called 'El Machete', which targeted a number of foreign countries, "would be consistent with the use of cyber capabilities for foreign intelligence purposes and would match Brazilian foreign and security policy interests." **Level 3**

Document	Excerpt
"Department of state international cyberspace policy strategy," US Department of State, March 2016.	The US international cyber strategy notes Brazil's emerging cyber capabilities in the same context as other known significant cyber actors including China and India. The collaborative relationship between the two countries was also highlighted. **Level 2**
"Deconstructing cyber security in brazil: Threats and Responses," Gustavo Diniz, Robert Muggah and Misha Glenny, December 2014.	This report indicated that the Brazilian army receives a considerable amount of money to develop cyber warfare capabilities, compared to law enforcement. It attributes this interest in military cyber partly to the espionage operations conducted against Brazil. The report begins by stating "although organized crime is one of the major threats to Brazilian cyberspace, resources are focused instead on military solutions better suited to the exceptional case of warfare." (P. 1) The report notes that "The extent of military preparation for cyber-warfare is not commensurate with the likely threat of armed conflict... the Brazilian government is preparing the armed forces to assume a leading role in the protection of Brazil's cyberspace, even though its primary use is civilian. There has been sizeable investment in upgrading military cyber capabilities..." (P. 23). **Level 3**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, October 5 2011.	This 2011 report identified significant Brazilian investment and interest in cyber capabilities. It also notes that, since 2010, Brazilian officials have taken part in US DoD sponsored cyber defence workshops. **Level 2**

Canada

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■◧□□

Organization for Offensive Cyber (2019): Communications Security Establishment

National Cyber Power Index (2020): Ranked 8th overall and 12th when it comes to offense

National Cybersecurity Index (2022) 66.23 (36th)

Internet Penetration (2020) 97%

Internet Freedom Score 87/100 (Free)

Transparency Description

Canada shows a high degree of transparency with regard to its offensive cyber capability. While not expressly detailing offensive capabilities, both the 2017 National Defence Policy and the 2018 Cyber Security Strategy refer to the government's intention to use active cyber operations to deter and respond to cyberattacks. In this regard, in 2019 Canada has established a dedicated unit within the Communications Security Establishment (CSE), Canada's SIGINT agency, tasked with conducting "active" cyber operations to disrupt the capabilities of foreign threats to Canada, such as: (i) foreign terrorist groups; (ii) foreign cyber criminals; (iii) hostile intelligence agencies; and (iv) state-sponsored hackers. While not offering specific details, in the 2021 Evaluation of Cyber Forces the Assistant Deputy Minister (Review Services) referred to active cyber operations and described the overall cyber programme, its design and desired outcomes. Canada's offensive cyber capabilities are largely perceived as to be under development, which is partly attributable to the relatively young mandate of the cyber force established in 2019. Several sources reported on the government's strong ambition and commitment to develop offensive capabilities. However, despite positioning 8th overall on the National Cyber Power Index, Canada ranks low when it comes to offensive capabilities.

Declared Capability Rating

Score ■■■□□

Canada has disclosed that it has offensive cyber capabilities. Given the short timeframe since its self-disclosure, details abouts its offensive branch is limited, which may be reflective of its maturity and that its public debate about cyber operations gained traction from 2017-2019 in the context of Bill C-59. Nonetheless, through the Performance Measurement and Evaluation Committee, the Canadian government already shows unique levels of transparency in the evaluation of its cyber forces.

Data availability rating (1 being highest number of sources, 10 lowest): **7/10**

Document	Excerpt
"Evaluation of the Cyber Forces," National Defence, April 2021.	Active cyber operations are mentioned in an evaluation of the cyber forces conducted by the Assistant Deputy Minister (Review Services). While it does not offer more details on offensive capabilities in particular, the report is very transparent about the overall cyber programme. It identifies challenges and recommendations on the programme design, delivery, and early initial outcomes. It includes details, such as the programme's expenditures, objectives, implementation and management, research and development, and personnel generation. Level 3

Document	Excerpt
"Bill C-59 : An Act respecting national security matters," House of Commons, June 21 2019.	Bill C-59, adopted in June 2019, describes the mandate and authorities for the Communications Security Establishment (CSE), Canada's SIGINT agency, to carry out active cyber operations: "[19] The active cyber operations aspect of the Establishment's mandate is to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security." Furthermore, "Active cyber activities would also have to be authorized by the Minister, with the consent of the Minister of Foreign Affairs or at the request of that Minister." **Level 3**
"National Cyber Security Action Plan 2019-2024," Public Safety Canada, June 2018.	The National Cyber Security Strategy does not directly address offensive capabilities but states the government's intention to use its capabilities to respond to and deter cyber-attacks: "In response to cyber threats of increasing sophistication, the Government of Canada will consider how its advanced cyber capabilities could be applied to defend critical networks in Canada and deter foreign cyber threat actors." (P.17) **Level 3**
"Strong, Secure, Engaged - Canada's Defence Policy 2017," National Defence, 2017.	In Canada's National Defence Policy, a reference is made to active cyber operations against potential adversaries, implying it had offensive capabilities: "We will assume a more assertive posture in the cyber domain by hardening our defences, and by conducting active cyber operations against potential adversaries in the context of government-authorized military missions." (P. 15) **Level 2.5**

Perceived Capability Rating

Score ■■■□□

Canada's offensive cyber capabilities are largely perceived to be nascent or under development, which is partly attributed to the relatively young mandate and the cyber force established in 2019. No public record is found on past Canadian cyber operations, with the exception of an operation that was attributed to a member of the Five Eyes community, to which Canada is a member.

Data availability rating (1 being highest number of sources, 21 lowest): **15/21**

Document	Excerpt
"Cyber Capabilities and National Power," IISS, June 28 2021.	"Canada is open about its ability and willingness to use offensive cyber [...].However, its offensive cyber capabilities are still nascent." (p. 43) "Historically, Canada's military cyber capabilities have tended to be defensive, and although other uses for cyber had already been envisaged in CAF/DND doctrine (the 2009 Capstone Concept, for example), it was only in 2019 that a cyber force was established in preparation for offensive cyber warfare." (p. 40) **Level 2**
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	While Canada was ranked 8th on this index, one of its worst performing areas was offence, where it was ranked 12th.

Document	Excerpt
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	"In some countries, overlapping organisations were created or reorganised over the course of several years," (P. 9) and notes Canada as such an example, pointing to the 2011 Directorate of Cybernetics which was "to build cyberwarfare capabilities," and conflicted with other departments. **Level 2**
"Zero D'Eh: Canada Takes a Bold Step Towards Offensive Cyber Operations," Stephanie Carvin, April 27 2018.	Notes that Canada's Bill C-59 would empower the Canadian signals intelligence agency (CSE) to engage in offensive cyber operations. **Level 2**
"Canada's Military Gets More Cyber, and the Headaches That Come With It," Alex Grigsby, June 22 2017.	Notes the Canadian government's recent public commitment to offensive cyber operations. It, however, questions how well they can implement this policy, stating that, at the very least, "It will take a few years for the Canadian Forces to build up their offensive capabilities and credibility." The author also notes that it's unclear how much new funding or personnel will be driven to developing this new offensive ability. **Level 1**
"Deconstructing cyber security in brazil: Threats and Responses," Gustavo Diniz, Robert Muggah and Misha Glenny, December 2014.	Mentions Canada, alongside the USA and the UK, as having committed online surveillance against Brazil, something Brazil saw as a 'cyber threat'. (P. 5) **Level 1**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, October 5 22 2011.	This 2011 report notes that prior to Bill C-59, the Canadian military cyber capabilities were mainly limited to electronic warfare and networks operations, currently known as Cyber and Electromagnetic Activities (CEMA). These activities are not the strategic cyber capabilities resulting from Bill C-59, but are directed at the tactical/operational level and mostly reserved to support military operations in the battlefield: "The Canadian army has an electronic warfare centre and a network operation centre, both of which support military cyber capabilities." (P. 8) **Level 2.5**

China

Cyber Transparency Score Untransparent

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■■■■

Organization for Offensive Cyber (2015): Strategic Support Force

National Cyber Power Index (2020): Ranked 2nd overall and 4th when it comes to cyber offense

National Cybersecurity Index (2022)	51.95 (62nd)
Internet Penetration (2020)	70%
Internet Freedom Score	10/100 (Not free)

Transparency Description

A lack of transparency is observed. China's foreign policy purportedly hinges on the doctrine of "peaceful use of cyberspace" and avoids the disclosure of details about its offensive cyber capabilities and forces. Nonetheless, the establishment of the Strategic Support Force (2015) and the Science of Military Strategy documents (2013a and 2015) allude to offensive capabilities as it aims to win 'informationised local wars and resolutely defend national territorial sovereignty, unity, and security". However, the structure, operative principles, and order of engagement governing cyber operations remain confidential. Despite the limited information officially disclosed, China is broadly perceived by other (mostly Western) states as possessing and using robust cyber offensive capabilities. Strong evidence in this regard may be inferred from the significant number of: (1) APTs affiliated to specific branches of Chinese military and intelligence agencies; (2) indictments issued against Chinese government officers and proxies; and (3) public attributions of Chinese cyber operations.

Declared Capability Rating

Score ■■■□□

China's foreign policy appears to underline the peaceful use of cyberspace, avoiding the disclosure of details about its offensive cyber capability. Prior to 2015, China had even strenuously denied and suggestions that it maintained official state cyber forces, despite the mountain of evidence to the contrary dating back to the 1990s. The publication of the 2013 and 2015 PLA Science of Military Strategy white papers, and the establishment of the Strategic Support Force in 2015 signaled that China has arrived in cyber offense. They often avoid using offensive language and instead cast their cyber capability in a defensive mold by using terms such as 'actively defending'.

Data availability rating (1 being highest number of sources, 10 lowest): **7/10**

Document	Excerpt
"《国家网络空间安全战略》全文 (National Cyber Security Strategy)," Cyberspace Administration of China, December 27, 2016.	"Guided by the overall national security concept, we will implement the development concept of innovation, coordination, green, openness, and sharing, enhance risk awareness and crisis awareness, coordinate the two major domestic and international situations, and coordinate the development of two major events, actively defending and responding effectively." [Original: 以总体国家安全观为指导，贯彻落实创新、协调、绿色、开放、共享的发展理念，增强风险意识和危机意识，统筹国内国际两个大局，统筹发展安全两件大事，积极防御、有效应对，推进网络空间和平、安全、开放、合作、有序，维护国家主权、安全、发展利益，实现建设网络强国的战略目标。] Level 0

Document	Excerpt
"The Science of Military Strategy," PLA, 2020.	"To meet the needs of building new types of forces such as digital forces, information operations forces, cyber operations forces, special operations forces, and cross-service construction forces, we must jointly establish comprehensive experimental and test bases to provide an experiment and test environment for the construction of new types of troops [...]" (p. 346) "Any warfare requires weapons, and the weapons for cyberspace warfare are quite special. Compared with traditional combat weapons which are hard kills, cyber weapons are soft kills in the form of computer software. With the militarization of confrontation in cyberspace, the means of confrontation in cyberspace has shifted to weaponization." (p. 404) "In cyberattack and defence, cyberspace attack is a stronger form of combat than cyberspace defence, and cyberspace attack capability is the core combat capability of cyberspace. Cyberspace attack capability refers to the penetration of the enemy's network system through information interference, information jamming, information destruction, etc., and the information left in the network by the enemy, or the host and the network system itself, to disrupt and destroy combat capability." (p. 405) "The core of network warfare capacity building is to train and possess a group of outstanding talents who are proficient in network warfare, that is, experts who are proficient in network technology and knowledgeable commanders who are familiar with network technology and are proficient in network warfare techniques and tactics. To seize the commanding heights of network confrontation, it is necessary to start early to train and bring up a large number of high-quality network confrontation talents who understand technology and precise tactics." (p. 412) **Level 3**
"China's Military Strategy," Ministry of National Defence PRC, May 26, 2015.	The Chinese Military Strategy emphasises "winning informationised local wars and resolutely defending national territorial sovereignty, unity and security." [Original: 基点放在打赢信息化局部战争上，坚决捍卫国家领土主权、统一和安全。] Furthermore, it claims that "Integrated combat forces will be employed to prevail in system-vs-system operations featuring information dominance, precision strikes, and joint operations." [Original: 运用诸军兵种一体化作战力量，实施信息主导、精打要害、联合制胜的体系作战。] **Level 2**
"The Science of Military Strategy," PLA, 2013.	The 2013 Science of Military Strategy of the PLA acknowledges cyberspace as an important war-fighting domain and refers to offensive cyber operations: "Main combat operations include: information offensive and defensive operations, offensive cyber and defensive operations. Major military deterrence operations include nuclear deterrence, conventional deterrence, space deterrence, and cyberspace deterrence."(P. 118) [Original: 主要作战行动包括：信息攻防，网空攻防行动主要的军事威慑行动包括核威慑，常规威慑，太空威慑和网络空间威慑。] **Level 3**

Perceived Capability Rating

Score ■■■■■

Viewed as having launched several successful offensive cyber operations, with the proven capability to disrupt and destroy enemy systems or infrastructure. Chinese offensive cyber operations have been widely reported on by other, mostly western, sources that primarily report on Chinese (economic) espionage operations carried out by state or non-state actors with a direct or indirect link to the government. They have expanded to more disruptive capabilities targeting critical infrastructure, which are integrated within the military structure (with the establishment of the Strategic Support Force) and the overall military planning and deterrence strategy. China is also perceived to further synchronise and develop its Cyber and Electromagnetic (CEMA) activities. Traditionally, PLA strategic thinking focused on 'information dominance' through operations targeting the adversary's command and control systems and using integrated information and firepower assaults. To this end, the PLA mostly concentrates on information operations that include cyber, electronic and psychological warfare components. In an effort to synchronise these operations, the Strategic Support Force (SSF) was established in 2015-16 as part of a massive PLA reform. It signified a significant push towards the militarisation of previously intelligence-driven PLA capacities, with the aim of developing more significant cyber *fires*.

Data availability rating (1 being highest number of sources, 21 lowest): **1/21**

Document	Excerpt
"The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China," The White House, July 19 2021.	US and allies attribute the 2021 Microsoft Exchange Server attack to the PRC: "Attributing with a high degree of confidence that malicious cyber actors affiliated with PRC's MSS conducted cyber espionage operations utilising the zero-day vulnerabilities in Microsoft Exchange Server disclosed in early March 2021." Joining the US in the attribution are the EU, the UK and NATO. **Level 3**
"Norway says cyber attack on parliament carried out from China," Nora Buli, July 19 2021.	Norway attribution of 2021 Parliament cyberattack to China: "Norway said that a March 10 cyberattack on parliament's e-mail system was carried out from China, calling on authorities there to take steps to prevent such activities". **Level 3**
"Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research," US Department of Justice, July 19 2021.	In 2021, the US Department of Justice indicted "four nationals and residents of the People's Republic of China with a campaign to hack into the computer systems of dozens of victim companies, universities and government entities in the United States and abroad between 2011 and 2018." Allegedly, three defendants "were officers in the Hainan State Security Department (HSDD), a provincial arm of China's Ministry of State Security (MSS)" **Level 3**
"Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," US Department of Justice, February 10 2020.	In 2020 the US Department of Justice indicted "four members of the Chinese People's Liberation Army (PLA) charged with hacking into the computer systems of the credit reporting agency Equifax and stealing Americans' personal data and Equifax's valuable trade secrets." **Level 3**
"Cyber Operations Tracker," Council on Foreign Relations, 2020.	The US-based Council on Foreign Relations's Cyber Operations Tracker lists China as having sponsored the most cyber operations (over 150 as per February 2022). **Level 5**
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	In the cyber power index, China was ranked second overall. China was ranked as 4th when it comes to cyber offence, lagging noticeably behind Russia, the UK and the US.
"Military and Security Developments Involving the People's Republic of China 2020," US Office of the Secretary of Defence, August 2020.	The US Department of Defence reported that one of the PLA's main goals is to be able to fight and win "informatised local wars", which appears to incorporate offensive cyber elements to achieve this state (P. 25). The Strategic Support Force (SSF) is identified as the main party responsible for military cyber operations (P. 61). In terms of the threat, it concludes that, while China believes it is still lagging behind the US, "the PRC presents a significant, persistent cyber espionage and attack threat to an adversary's military and critical infrastructure systems." (P. 81). The latter serves to establish some form of deterrence and past targets include the US DoD (P. 83-84). It also notes that the PLA is developing its cyber and electronic activities (CEMA), such as "satellite jammers; offensive cyber capabilities; and directed-energy weapons," (P. 65). **Level 4**
"Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax," US Department of Justice, February 10 2020.	US attribution of 2014 OPM breach, 2015 Anthem breach, the 2017 Equifax breach and the 2018 Marriot hotels breach to China: in a press release on the indictment of four PLA officers for the Equifax breach, Attorney General Barr stated that "for years, we have witnessed China's voracious appetite for the personal data of Americans, including the theft of personnel records from the U.S. Office of Personnel Management, the intrusion into Marriott hotels, and Anthem health insurance company, and now the wholesale theft of credit and other information from Equifax." **Level 3**
"Worldwide Threat Assessment of the US Intelligence Community," Daniel R. Coats, January 29 2019.	The US Intelligence Community report emphasised the threat from Chinese cyber-enabled IP theft and its ability to potentially launch disruptive cyberattacks against US critical infrastructure: "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies. It is improving its cyberattack capabilities and altering information online, shaping Chinese views and potentially the views of US citizens." [...] "China has the ability to launch cyberattacks that cause localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States." (P. 5). **Level 4**
"U.S., allies slam China for economic espionage, spies indicted," Diane Bartz, Jack Stubbs, December 20 2018.	US, UK, Australia and Zealand attribute a 2018 global cyber espionage campaign to China: "Britain, Australia and New Zealand joined the United States in slamming China over what they called a global campaign of cyber-enabled commercial intellectual property theft, signaling growing global coordination against the practice." **Level 1**
"Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," US Department of Justice, October 30 2018.	In 2018 the US Department of Justice indicted several Chinese intelligence officers and their subordinates, including hackers and company insiders, that "conducted or otherwise enabled intrusions into private companies' computer systems in the United States and abroad for over five years". The charged individuals worked for the Jiangsy Province of the Ministry of State Security. **Level 3**

Document	Excerpt
"A Guide to Cyber Attribution," Office to the Director of National Intelligence, September 14 2018.	Identifies China as one of the prominent malign actors that uses "cyber operations as a low-cost tool to advance their interests..." (P. 2). Specifically uses the example of Chinese cyber-enabled IP theft (P. 5). **Level 3**
"The Darkening Web: The War for Cyberspace," Alexander Klimburg, 2017.	"Besides the sheer scale of the PLA cyber force, the truly remarkable element is how long it has been in existence. There are indications that the 3PLA Second Bureau, one of the most active attackers against the United States, was already set up in 1995. Although it is unclear whether the Second Bureau already had a specific cyber mission, the sheer longevity of the command probably makes it one of the longest-standing cyber units in the world [...] The US Army scholar Timothy Thomas, for instance, wrote as far back as 2004 about the Guangzhou information warfare militia battalion that had specific companies for computer network operations and electronic warfare" (P. 285) **Level 4**
"Remembering Operation Titan Rain," Cyware, October 27 2016.	US attribution of 2003 operation Titan Rain to China: Cyware's article mentions speeches and unclassified US documents that identify a link between the hackers and the Chinese government. **Level 3**
"Chinese National Who Conspired to Hack into U.S. Defense Contractors' Systems Sentenced to 46 Months in Federal Prison," US Department of Justice, July 13 2016.	In 2016 the US Department of Justice sentenced a "Chinese national who admitted to participating in a years-long conspiracy that involved Chinese military officers hacking into the computer networks of major U.S. defence contractors in order to steal military technical data". The individual admitted his role "with hackers from the People's Liberation Army Air Force to illegally access and steal sensitive US military information" **Level 3**
"China blamed for 'massive' cyber attack on Bureau of Meteorology computer," Chris Uhlmann, December 2 2015.	Australian attribution of 2015 Bureau of Meteorology cyberattack to China: according to the media, "the ABC has been told this is a "massive" breach and one official said there was little doubt where it came from. "It's China," he said. (...) Australian Strategic Policy Institute (ASPI) executive director Peter Jennings said there was evidence China was behind the hack." **Level 3**
"SASC investigation finds Chinese intrusions into key defense contractors," US Senate Committee on Armed Services, September 17 2014.	US attribution of 2014 TRANSCOM cyberattack to China: the United States Senate Committee on Armed Services published a press release stating that "Hackers associated with the Chinese government successfully penetrated the computer systems of U.S. Transportation Command contractors at least 20 times in a single year, intrusions that show vulnerabilities in the military's system to deploy troops and equipment in a crisis. **Level 1**
"Chinese cyberattack hits Canada's National Research Council," Rosemary Barton, July 30 2014.	Canadian attribution of 2014 National Research Council cyberattack to China: according to Canada's Chief Information Officer at the time, Corinne Charette, "a "highly sophisticated Chinese state-sponsored actor" recently managed to hack into the computer systems at Canada's National Research Council". **Level 3**
"U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," US Department of Justice, May 19 2014.	US attribution of 2014 Westinghouse Electric and US Steel Corporation hacking to China: "A grand jury in the Western District of Pennsylvania (WDPA) indicted five Chinese military hackers for computer hacking, economic espionage and other offenses directed at six American victims in the U.S. nuclear power, metals and solar products industries." The DOJ press release specifies that the defendants were officers in Unit 61398 of the Third Department of the Chinese PLA. **Level 3**
"White House Hack Attack," Bill Gertz, September 30 2012.	US attribution of 2012 White House cyberattack to China: "Hackers linked to China's government broke into one of the U.S. government's most sensitive computer networks, breaching a system used by the White House Military Office for nuclear commands, according to defense and intelligence officials familiar with the incident." **Level 3**
"China Hackers Hit U.S. Chamber," Siobhan Gorman, December 21 2011.	US attribution of 2011 US Chamber of Commerce hack to China: according to an article published on the Wall Street Journal "the group behind the break-in is one that U.S. officials suspect of having ties to the Chinese government. The Chamber learned of the break-in when the Federal Bureau of Investigation told the group that servers in China were stealing its information." (medium) **Level 3**
"2011 Report to Congress of the U.S.-China Economic and Security Review Commission," US Government, November 2011.	US attribution of 2008 NASA attacks to China: the 2011 US-China Economic and Security Review Commission report to Congress a China states that the NASA attacks "techniques appear consistent with authoritative Chinese military writings." **Level 3**
"2011 Report to Congress of the U.S.-China Economic and Security Review Commission," US Government, November 2011.	US attribution of 2011 RSA compromise to China: the 2011 US-China Economic and Security Review Commission report to Congress a China affirms that in the RSA SecurID compromise "the perpetrators then used information about compromised RSA security product in order to target a number of the firm's customers, including at least three prominent entities within the U.S. defense industrial base. Those intrusions and intrusion attempts, according to some reports, also originated in China and appeared to be state sponsored". **Level 3**

Document	Excerpt
"China logs in to hack PMO: NSA," The Economic Times, January 19 2010.	Indian attribution of 2010 attempt to hack the Prime Minister's Office: National Security Advisor at the time, M K Narayanan, said in an interview that "people seem to be fairly sure it was the Chinese. It is difficult to find the exact source but this is the main suspicion. It seems well founded". (medium) **Level 3**
"Hackers Based in China Break Into Florida Senator's Office Computers," Josh Rogin, March 20 2009.	US attribution of 2009 Senator Nelson computers compromise to Chinese government: a website reports that "some officials have admitted that they suspect the Chinese government is behind the attacks, due to the level of sophistication and the nature of the information targeted." The level of attribution is quite weak as no official statement by US authorities was released and the officials were anonymized. **Level n/a**
"Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," Brian Krekel, October 9 2009.	A report for the US-China Economic and Security Review Commission detailing China's cyber warfare capabilities. One of its conclusion is that "In a conflict with the US, China will likely use its CNO capabilities to attack select nodes on the military's Non-classified Internet Protocol Router Network (NIPRNET) and unclassified DoD and civilian contractor logistics networks in the continental US (CONUS) and allied countries in the Asia-Pacific region. The stated goal in targeting these systems is to delay US deployments and impact combat effectiveness of troops already in theater." (P. 8). This capability has evolved since 2009. **Level 4**
"Chinese military hacked into Pentagon," Demetri Sevastopulo and Richard McGregor, September 3 2007.	US attribution of US officials of 2007 Pentagon hack to Chinese PLA: "current and former officials have now told the Financial Times that an internal investigation into the attack has revealed it came from the People's Liberation Army" **Level 1**
Attribution to PLA:	
APT 12 (aka numbered Panda, DYNCALC, IXESHE, JOY RAT, DNSCALC, G-2754, BeeBus, Group 22, Calc Team, Crimson Iron, BRONZE GLOBE) "Darwin's Favorite APT Group," Ned Moran and Mike Oppenheim, September 3 2014. (1) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (2)	APT 12 is a cyber espionage group thought to have links to the Chinese People's Liberation Army. Its targets fall in line with the People's Republic of China objectives. A recurrent target is the Taiwanese government, with several recorded spear-phishing campaigns including "RipTide" in October 2012, "HighTide," "Threebyte," and "Waterspout" in August 2014. Another important operation took place in October 2012 when the group breached the New York Times after the media outlet published an article on Chinese premier minister Wen Jiabao. **Level 1**
APT17 (aka Elderwood, Sneaky Panda, Elderwood Gang, SIG22, Bejing Group) "Blurred Lines Between State and Non-State Actors," CFR, December 5 2019. (1) "Hiding in Plain Sight: Fireye and Microsoft Expose Obfuscation Tactic," Fireye, May 2015. (2)	APT17 is a group that has in the past compromised US government networks as well as networks in the defence industry, law sector, IT and mining enterprises and non-governmental organizations. Although the group has been linked to the Jinan Bureau of China's intelligence agency, the Ministry of State Security (MSS), it is also known to have carried out cybercrime for monetary gain against the Chinese population. **Level 1**
APT (Naikon) (aka Lotus Panda, Hellsing) "Project CameraShy: Closing the Aperture on China's Unit 78020," ThreatConect, 2019. (1) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (2)	APT (Naikon), found to be behind cyberespionage operations, has been attributed to the People's Liberation Army (Unit 78020). Its intelligence gathering operations focused around targets linked to the South China Sea. These include government bodies in Cambodia, Indonesia, Laos, Malaysia, Myanmar, Nepal, the Philippines, Singapore, Thailand, and Vietnam as well as international organisations like the United Nations Development Programme (UNDP) and the Association of Southeast Asian Nations (ASEAN). Its recent activity involves a 2014 campaign against actors investigating the disappearance of MH37, Operation "Camera Shy" linking PLA member Ge Xing to spear phishing campaigns against South-East Asian military, diplomatic and economic entities in 2015 and various operations in 2017 against targets in the Asia Pacific region. **Level 1**
APT 2 (aka Putter Panda, TG-6952, Group 36, Sulphur, MSUpdater) "CrowdStrike Intelligence Report: Putter Panda," Crowdstrike, June 9 2014.	APT 2, a group linked to the PLA (Unit 61486), conducts intellectual property theft operations against research companies and satellite, aerospace and communication enterprises, mainly in the US and in Europe. **Level 1**
APT 14 (aka Anchor Panda, Aluminum, QAZTeam) "Advanced Persistent Threat Groups," Mandiant, last accessed February 2022.	APT 14, a group connected to the PLA Navy, specialises in information theft against Western companies developing maritime satellite systems, aerospace companies, and defence contractors. **Level 1**

Document	Excerpt
APT 18 (aka Dynamite Panda, TG-0416, Wekby, Scandium) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	APT 18 is thought to be linked to the PLA Navy but little information has been released on it. Operations involve intelligence-gathering from the healthcare, telecommunications, aerospace, defence, and high tech sectors. The group is responsible for the Community Health Systems data breach in 2014, stealing patient information from a hospital in the US. Since then, the group has carried out campaigns against various US-based organisations. **Level 1**
APT (DragonOK) (aka Samurai Panda, Temp.DragonOK, BRONZE OVERBROOK) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group, with suspected affiliation to the PLA Navy, has carried out a number of phishing campaigns against Japanese entities. Its operations include a 2015 campaign against a Japanese manufacturing company, various recorded campaigns throughout 2016 against Japan (and to a lesser degree Taiwan, Tibet, and Russia) and a 2017 campaign against organisations in Cambodia. **Level 1**
APT 4 (aka Maverick Panda, Sykipot Group, Wisp, TG-0623, BRONZE EDISON) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Cryptocurrency firms are targets of state-sponsored hacking group from China," Suvajit Banerjee, August 8, 2019. (2)	APT 4, a group linked to the PLA Navy, is known for carrying out cyberespionage operations against the Defence Industrial Base (DIB) but have also given priority to intelligence-gathering campaigns in the telecommunications, computer hardware, government contractors, and aerospace sectors. Its recent operations include a 2013 campaign targeting US Civil Aviation Sector Information, a 2015 breach of an Asian airline company and 2018 campaigns against gaming start-ups last year and a cryptocurrency exchange. **Level 1**
APT 10 (aka Dust Storm, DustStorm, ATK41, Cloud Hopper, Happyyongzi, Hogfish, Menupass, Potassium, Red Apollo, Stone Panda, CVNX, menuPass Team, BRONZE RIVERSIDE, CTG-5938, CNVX) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	APT10 is a cyberespionage group attributed to Tianjin bureau of the Chinese Ministry of State Security and Huaying Haitai Science and Technology Development Company. Their main focus is on intellectual information theft from construction and engineering, aerospace, and telecom companies. In 2016, the group targeted "Japanese academics working in several areas of science, along with Japanese pharmaceutical and a US-based subsidiary of a Japanese manufacturing organizations" (P. 310) in a spear-phishing campaign. In 2016, another two parallel operations were recorded, one compromising IT service providers and their clients dubbed Operation "Cloud Hopper", and another one against Japanese organisations. In 2016 and 2017, operations against manufacturing companies in India, Japan and Northern Europe; a mining company in South America; and numerous IT service providers were detected. In 2017, Operation "TradeSecret" compromised The National Foreign Trade Council (NFTC) network; Operation "ChessMaster"targeted Japanese academe, technology firms, media, managed service providers, and government bodies; and Operation "Soft Cell" attacking communication providers worldwide. In November 2017 an information theft operation was uncovered against a Norwegian firm, IT and business cloud services managed service provider and a US law firm. In 2018, the group conducted a campaign against the Japanese media sector. Finally, in 2019 the group breached aerospace corporation Airbus' information systems. **Level 3**
APT (Bronze Butler) (aka Tick, RedBaldNight, Stalker Panda, TEMP. Tick) "BRONZE BUTLER Targets Japanese Enterprises," Secureworks, October 12 2017. (1) "Operation ENDTRADE: TICK's Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data," Joey Chen, Hiroyuki Kakara, and Masaoki Shoji, November 29 2019. (2)	APT Bronze Butler is linked to the National University of Defence and Technology as well as the PRC and its activity mainly revolves around intellectual property theft from Japanese organisations, notably in the critical infrastructure, heavy industry, manufacturing, and international relations sector. In 2018, the group carried out Operation "ENDTRADE" stealing proprietary and confidential data from Japanese organisations mainly in the defence and chemical sector. In 2019, manufacturing company Mitsubishi Electric disclosed a breach attributed to APT Bronze Butler. **Level 1**
APT 3 (aka Gothic Panda, Buckeye, UPS Team, TG-0110, Boyusec, BORON, BRONZE MAYFAIR) "Buckeye: Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak," Symantec, May 7 2019. (1) "Clandestine Fox, Part Deux," Mike Scott, June 10 2014. (2)	APT 3 has been attributed to the Chinese National University of Defence and Technology, the Ministry of State Security and Guangzhou Bo Yu Information Technology Company Limited ("Boyusec"). Its sophisticated intelligence-gathering attacks have been known to target defence, telecommunications, transportation, non- profit and high tech sectors as well as government bodies in Hong Kong and the US. In 2014, the group were thought to be the actors of Operations "Clandestine Fox," a spear-phishing campaign against an energy company according to Fireeye (June 2014). In November of the same year, the Operation "Double Tap" was uncovered targeting several organisations. In 2015, the group targeted the Aerospace and Defence, Construction and Engineering, High Tech, Telecommunications and Transportation sectors. In 2016, the group used Equation Group tools against a target in Hong Kong and in September of the same year to attack a Hong Kong educational institution. **Level 4**

Document	Excerpt
APT 26 (aka Hippo Team, JerseyMikes, Turbine Panda, BRONZE EXPRESS, TG-0055) "Intelligence Report: Huge Fan of Your Work: How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet," CrowdStrike, October 2019. (1) "Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years," US Department of Justice, October 30 2018. (2)	APT 26, attributed to Jiangsu Ministry of State Security (JSSD), specialises on sensitive information theft from aviation companies. For instance, in 2010 the group targeted Capstone Turbine Corporation, a US-based gas turbine manufacturer. A report by CrowdStrike (2) mentions that between 2010-2015 other firms aerospace-related were targeted, notably Honeywell and Safran. The intellectual property stolen was later used by China to manufacture a C919 Passenger Jet, according to the report. **Level 1**
Potential attribution to PLA Unit 65017 - APT (Tonto Team) (aka CactusPete, Karma Panda, HartBeat, HeartBeat, LoneRanger, Team Tonto, BRONZE HUNTLEY, Bisonal) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "Researchers claim China trying to hack South Korea missile defense efforts," Sean Gallagher, April 21 2017 (2)	First discovered in 2009, APT (Tonto Team) carries out politically-motivated cyberespionage operations. In fact, it is potentially linked to Shenyang Military Region Technical Reconnaissance Bureau, possibly Unit 65017. Its targets comprise entities related to the South Korean government. Specifically political parties, media, a national policy research institute, a military branch of the South Korean armed forces, small businesses and branches of the South Korean government. In 2017, Fire Eye reported on a Chinese campaign against South Korean defence, military and government bodies. This was in response the use of Terminal High-Altitude Air Defence (THAAD) by South Korea for defence purposes against the DPRK. **Level 1**
APT (RedAlpha) "Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community," Masashi Crete-Nishihata, Jakub Dalek, Etienne Maynier, and John Scott-Railton, January 30 2018.	APT Red Alpha is potentially linked to the Chinese PLA and/or the Nanjing Qinglan Information Technology Co. Its only recorded operation was a 19-month spear phishing campaign targeted at Tibetan actors in India–journalists, activist and members of the Central Tibetan Administration among others – in 2017. **Level 1**
APT 40 (aka Leviathan, TEMP. Periscope, TEMP.Jumper, Bronze Mohawk, Mudcarp, ATK29, Flaccid Rose, Kryptonite Panda, GADOLINIUM, Nanhaishu, Pickleworm) "Leviathan," Mitre Att&ck, April 18 2018. (1) "Leviathan: Espionage actor spear-phishes maritime and defense targets," Proofpoint, October 16 2017. (2) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (3)	According to Mitre Att&ck, APT 40 has been attributed to the "Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company" (1). It has been active since at least 2013 and executes cyber espionage operations against engineering, transportation, and the defence industry likely in order to advance China's naval force. For example, in 2014, a number of attacks were uncovered against defence contractors, universities with military ties, legal organisations and government bodies, all somehow related to the naval sector. In 2017, the group carried out a spear phishing campaign against a British engineering company and continued to target American entities involved in the naval sector. However, most recently the group seems to have change its focus to target countries with strategic importance in the Road and Belt initiative, notably Cambodia, Belgium, Germany, Hong Kong, Philippines, Malaysia, Norway, Saudi Arabia, Switzerland, the United States, and the United Kingdom. For instance, in 2018, APT 40 targeted individuals in the opposition and organisations in Cambodia involved in the electoral process around the time of the general elections. Moreover, in 2020, Malaysian government-backed organisation denounced an increase in campaigns targeting Malaysian officials. **Level 3**
APT (Lotus Blossom) (aka Spring Dragon, Dragonfish, Elise, ATK1, ST Group, Bronze Elgin, Billbug) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "Thrip: Ambitious Attacks Against High Level Targets Continue," Broadcom, September 9 2019 (2)	Active since at least 2012, the group is likely attributed to the Chinese state. Its main focus is high profile governmental entities, political parties, research universities and the telecommunications sector in countries around the South China Sea. Operation Lotus Blossom (2015-2017) is a long standing cyberespionage campaign that targets Southeast Asian military and governmental organisations. Throughout 2018, the group targeted ASEAN countries in a malware spam campaign and launched operations against military organisations and the maritime communication, satellite communication, media and education sectors. As of 2019, the group was still targeting satellite communication organisations. **Level 1**
APT (Mofang) (aka Superman, BRONZE WALKER) "Mofang: A politically motivated information stealing adversary," Fox It, May 17 2016. (1) "Whitefly: Espionage Group has Singapore in Its Sights," Broadcome, March 6 2019. (2)	The APT Mofang has been active since at least 2012 and is likely sponsored by the Chinese government. The group targets various sectors (government, military, critical infrastructure and the automotive and weapon industries) in different countries (India, Germany, United States, Canada, Singapore, South Korea) but is known for selecting its targets "based on involvement with investments, or technological advances that could be perceived as a threat to the Chinese sphere of influence" ((1) P.2). For instance, the group targeted a Burmese company with investments in a territory of strategic interest for China's National Petroleum Corporation's investments. In another instance (2018), the group stole information from SingHealth, Singapore's largest public health organisation. The group retrieved sensitive medical information on 1.5 million individuals. **Level 1**

Document	Excerpt
APT (BRONZE PRESIDENT) (aka HoneyMyte, Mustang Panda, Red Lich, Temp.Hex) "BRONZE PRESIDENT Targets NGOs," Secureworks, December 29 2019 (1) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (2)	APT BRONZE PRESIDENT, likely sponsored by the PRC, was first detected in a 2017 campaign targeting US think tanks. After more examination it was revealed that the group, likely to be state sponsored by China, targets NGOs, using Mongolian content as bait. This suggests that the objective of the operations is to gather information on Mongolian victims. In 2020, a number of campaigns were detected: an espionage operations against victims in Vietnam and Hong Kong, and various attacks against Vietnamese target with Covid19 content to lure victims. **Level 1**
APT 9 (aka Nightshade Panda, APT 9, Group 27, Flowerlady, Flowershow) (potentially freelancers sponsored by the Chinese state) "Advanced Persistent Threat Groups," Mandiant, January 21 2022 (1). "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (2)	According to Mandiant, APT 9 is a freelancer group possibly sponsored by China (1). The group usually targets the health care and pharmaceuticals, construction and engineering, and aerospace and defence sectors in various countries. In May 2015, the group infected visitors of the official President of Myanmar's website ahead of the elections. During the same month, the group also carried out a spear phishing campaign against the US government and a EU media company. Between September and November 2016, the group "compromised two Thai websites to host malware." **Level n/a**
APT 23 (aka Pirate Panda, KeyBoy, Tropic Trooper, BRONZE HOBART) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "It's Parliamentary: KeyBoy and the targeting of the Tibetan Community," Adam Hulcoop, Matt Brooks, Etienne Maynier, John Scott-Railton, and Masashi Crete-Nishihata, November 17 2016. (2)	APT 23, possibly linked to the Chinese state, usually carries out traditional intelligence gathering operations against government and military targets. In 2012, a campaign dubbed Operation Tropic Trooper was uncovered, targeting the Taiwanese government and Philippine's military entities. This campaign continued through 2013-2015, also targeting Hong Kong and the healthcare, transportation, and high-tech industries. In 2016, the group launched an espionage campaign against members of the Tibetan Parliament. In 2020, it was uncovered that the group was targeting officials of the Vietnamese government through spear-phishing emails. **Level n/a**
APT (Platinum) (aka TwoForOne, ATK33) "PLATINUM Targeted attacks in South and Southeast Asia," Microsoft, April 29 2016. (1) "Platinum is back," Securelist, June 5 2019. (2)	The group, active since at least 2009, focuses on information theft. It is possibly linked to China. Its targets are "opportunistic" ((1) P.4). According to Microsoft, "the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world" ((1) P.4). It generally targets governments, diplomatic bodies and telecommunication companies in South and Southeast Asia. For example in 2016, it targeted a legitimate Indian website which offered an email service to its users. It then sent spear phishing emails to the users among which there were government officials. In this way, it attempted to gain control of high-profile target's computers. In 2018, Securelist identified a long standing campaign against diplomatic, government and military entities in South and Southeast Asian countries. **Level n/a**
APT (Rancor) (aka Rancor Group) "Rancor: The Year of The Phish," Check Point, September 22 2019	The group has been active since at least 2017 and is potentially attributable to China. Between 2018 and 2019 APT Rancor was found to be carrying out a 7 month spear-phishing campaign against Southeast Asian government organizations. **Level n/a**
APT (Roaming Tiger) (aka BRONZE WOODLAND, CTG-7273, Rotten Tomato) "BBSRAT Attacks Targeting Russian Organizations Linked to Roaming Tiger," Bryan Lee and Josh Grunzweig, December 22 2015.	Roaming Tiger is possibly state-sponsored by China and active since at least 2014. It targets high-profile Russian targets and Russian speaking nations. In August 2015, Paloalto uncovered attacks exploiting a Microsoft Office vulnerability to take control of the victim's computer. **Level n/a**
APT (Shadow Network) "SHADOWS IN THE CLOUD: Investigating Cyber Espionage 2.0," Information Warfare Monitor, April 6 2010.	According to Citizen Lab, Shadow Network is a "complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries," (P.4) likely linked to the PCR. The group steals highly sensitive information, for instance encrypted documents suspected to be from the Indian government or letters sent from the Dalai Lama's office in 2009. **Level n/a**

Document	Excerpt
APT (Scarlet Mimic) "Scarlet Mimic: Years-Long Espionage Campaign Targets Minority Activists," Robert Falcone and Jen Miller-Osborn, January 24 2016.	The group is known for targeting minority right groups and those sympathetic to them, notably Uyghur and Tibetan activists as well as a Turkic Muslim minority residing primarily in northwest China. The targets seem to align with Chinese interests and the group's IP also overlaps with that of Putter Panda and APT 2. Therefore, the group could possibly be linked to the PRC. The latest recorded operation was an information gathering campaign against Indian and Russian organisation that track activist and terrorist activities in their respective countries. The group had a specific interest in Muslim activists and activists critical of Putin. **Level n/a**
APT (Gallium) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	APT Gallium was first uncovered by Microsoft in 2018. It is possibly linked to China and carries out espionage operations against the telecommunications sector. Although it remains active, its activity has gone in decrease since 2019. **Level n/a**
APT (Operation Shady RAT) "Revealed: Operation Shady RAT," McAfee, March 2011.	The group, active since at least 2006, is thought to be sponsored by China. The group has targeted multiple sectors in multiple countries. The McAfee report lists some of its operations: "In 2006 (...) we saw only eight intrusions: two on South Korean steel and construction companies, and one each on a South Korean Government agency, a Department of Energy Research Laboratory, a U.S. real-estate firm, international trade organisations of an Asian and Western nations and the ASEAN Secretariat" (P.6) (...) "In 2007, the pace of activity jumped by a whopping 260 percent to a total of 29 victim organizations(...) four U.S. defense contractors, Vietnam's government-owned technology company, US federal government agency, several U.S. state and county governments, and one computer network security company. The compromises of the Olympic Committees of two nations in Asia and one Western nation began that year as well. In 2008, the count went up further to 36 victims, including the United Nations and the World Anti-Doping Agency, and to 38 in 2009. Then the number of intrusions fell to 17 in 2010 and to 9 in 2011, likely due to the widespread availability of the countermeasures for the specific intrusion indicators used by this specific actor" (P.6). **Level n/a**
APT (PKPlug) (aka HenBox, Farseer) "PKPLUG: Chinese Cyber Espionage Group Attacking Southeast Asia," Alex Hinchliffe, October 3 2018.	The group is known for targeting Myanmar, Taiwan, Vietnam, and Indonesia; and likely also in various other areas in Asia, such as Tibet, Xinjiang, and Mongolia. The targets align with the PCR's interests thus, it is possible that PKPlug is state-sponsored. Most of the countries are part of ASEAN, are involved the Belt and Road Initiative and/or have some involvement in the South China Sea issue, both strategically important to China. In November 2013, Blue Coats Lab uncovered an attack against Mongolian or Mongolian-related targets. In 2016 activity was reported against Myanmar in two instances: one using ASEAN issues as bait and another using information on Myanmar activists. In 2017, spear-phishing against Japan and Myanmar were recorded. In 2018, Unit 42 discovered a campaign that used a malicious Android app to target Uyghurs and a minority Turkic group living in Northwest China. The latest recorded activity in February 2019 employed decoy documents on Myanmar political news for the attack. **Level n/a**
APT (SabPub) "SabPub Mac OS X Backdoor: Java Exploits, Targeted Attacks and Possible APT link," Securelist, April 12 2014.	On the attacks, Securelist reports: "This new threat is a custom OS X backdoor, which appears to have been designed for use in targeted attacks. After it is activated on an infected system, it connects to a remote website ... to fetch instructions. The backdoor contains functionality to make screenshots of the user's current session and execute commands on the infected machine." "Several reports exist which suggest the attack was launched through e-mails containing an URL pointing to two websites hosting the exploit, located in US and Germany. The timing of the discovery of this backdoor is interesting because in March, several reports pointed to Pro-Tibetan targeted attacks against Mac OS X users. The malware does not appear to be similar to the one used in these attacks, though it is possible that it was part of the same or other similar campaigns." Because the attacks align with Chinese interests, it is possible that the group is state-sponsored. **Level n/a**
APT (BRONZE DUDLEY) (aka Vicious Panda) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	A campaign by BRONZE DUDLEY in 2020 employing information on Covid19 to attack the Mongolian public sector uncovered past operations carried out by the same APT. In 2015, the group utilised phishing emails and infected legitimate-looking documents against the offices of the Mongolian government. In 2017, another similar campaign was carried out but this time against Belarussian government entities. Because the attacks align with Chinese interests, it is possible that the group is state-sponsored. **Level n/a**
APT (BlackTech) (aka CIRCUIT PANDA, Temp.Overboard, HUAPI, Palmerworm, T-APT-03) "Waterbear Returns, Uses API Hooking to Evade Security," Vickie Su, Anita Hsieh, Dove Chiu, December 11 2019 (1) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (2)	Black tech is a cyberespionage group thought to be linked to the Chinese state. Its targets are countries in East Asia, especially Taiwan and to a lesser extent Japan and Hong Kong. For example, Operation PLEAD in 2012 targeted Taiwanese government bodies and private entities. In 2018, the group employed stolen digital certificates to launch a malware attack against Taiwanese security company Changing Information Technology Inc. Most recently, in 2019, a APAC-based security vendor was also targeted by BlackTech. **Level n/a**

Document	Excerpt
Suspected affiliation to the Chinese State	
APT 5 (aka Maganese, Bronze Fleetwood, Keyhole Panda, DPD, Poisoned Flight, TG-2754) "Advanced Persistent Threat Groups," Mandiant, January 21 2022. (1) "A Chinese APT is now going after Pulse Secure and Fortinet VPN servers," Catalin Cimpanu, September 5 2019. (2)	The group has been active since at least 2007 and is thought to be sponsored by China. It seems to be an umbrella organization with various subgroups and a variety of tactics. APT 5 has a broad range of targets but seems to target telecommunications and technology companies, especially information about satellite communications more often. In 2015, the group breached a US telecommunications company that sold services and technology to the government and private entities. In the same year, the group stole information relating to military technology form a South Asian defence body. In the 2019, the group attempted to exploit vulnerabilities in the PulseSecure and Fortinet VPN servers to steal files with password information and other sensitive data. **Level 1**
APT 17 (aka Deputy Dog, Tailgater Team, Dogfish, ATK2, Axiom, Blackfly, Group 72, Group 8, Hidden Lynx, Lead, Ragebeast, Sneaky Panda, Aurora Panda, BRONZE KEYSTONE, Shell Cre, Tailgater Team) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "Operation RAT Cook: Chinese APT actors use fake Game of Thrones leaks as lures," Darien Huss and Matthew Mesa, August 25 2017. (2) "CCleanup: A Vast Number of Machines at Risk," Talos, September 18 2017. (3)	The group, first detected in 2009, is thought to be linked to the Jinan bureau of the Chinese Ministry of State Security. It specialises in information gathering and intellectual property theft form a range of industries: defence, defence supply chain manufacturers, human rights and non-governmental organisations (NGOs), and IT service providers. In 2009, the group carried out Operation Aurora, an attack first reported by Google but also targeting other firms like Adobe Systems, Juniper Networks and Rackspace. In 2010, the group compromised the network of US defence contractor firm Lockheed Martin Corp LMT.N. Between 2010 and 2012, APT 17 carried out attacks against users visiting the page of Amnesty International in Hong Kong and in the UK. In July 2012, the group breached Bit9, a firm that sells network and software security services to the US government and other high-profile companies. In 2013, Operation Ephemeral Hydra, compromised website focused on national and international security policy. In 2017, the group authored Operation RAT Cook, a spear phishing attack using previews of the new Game of Thrones season as bait. In 2019, Talos detected supply chain attack where CCleaner 5.33 software by Avast contained malware in its installation. **Level 1**
APT 19 (aka C0d0so, Codoso, Codoso team, Sunshop Group, Deep Panda, Shell Crew, WebMasters, KungFu Kittens, Group 13, PinkPanther, Black Vine, Sh3llCr3w, BRONZE FIRESTONE) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020	The group, active since at least 2013, is thought to be formed by freelancers with some sponsorship from the Chinese state. They usually target the legal and investment sectors as well as the US government. In March 2014, the group compromised the network of the US Office of Personnel Management OPM. In the same month, the group also breached USIS, a background check provider for the U.S. Department of Homeland Security. Later that year, other targeted operations were uncovered against the U.S. Defence Industrial Base (DIB), healthcare, government, and technology sectors. In December of the same year, KeyPoint Government Solutions uncovered a breach in its system, likely attributed to APT 19. In April 2015, the group authored a supply chain attack with software usually used by enterprise system administrators. A month later, a number of breaches were detected on health insurance companies in the US. In May 2017, a large scale phishing campaign was recorded against law and investment firms worldwide. **Level 3**
APT 20 (aka Violin Panda, APT 8, TH3Bug, Operation Wocao, Twivy) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "Operation Wocao Shining a light on one of China's hidden hacking groups," Maarten van Dantzig & Erik Schamper, December 19 2019. (2)	The group, active since 2014, is known for compromising legitimate websites in watering hole attacks. The websites are usually somehow related to Chinese interests thus it is likely that the group is sponsored by the Chinese government. The target sectors include aviation, energy, finance, health care, offshore engineering, software development, transportation, among others. The group is known to have attacked at least 10 countries worldwide. For example, in 2014 they compromised legitimate websites written in the Uyghur language. **Level 3**
APT 30 (aka Override Panda, BRONZE STERLING, BRONZE GENEVA, CTG-5326, Naikon) "APT30 and the Mechanics of a Long-running Cyber Espionage Operation," FireEye, April 2015.	The group has been executing intelligence gathering operations for over a decade and it is likely linked to the Chinese government. Its targets include organisations and governments associated to the ASEAN. In fact, activity is intensified before ASEAN meetings. In addition, this group has also targeted in the past journalists undermining the credibility of the Chinese Communist Party by reporting on corruption or human rights. **Level 1**

Document	Excerpt
APT 41 (aka Axiom, Winnti Umbrella, Winnti Group, Suckfly, Barium, Pigfish, APT41, Group72, Group 72, Blackfly, LEAD, WICKED SPIDER, WICKED PANDA, BARIUM, BRONZE ATLAS, BRONZE EXPORT, Red Kelpie) (hacker-for-hire) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "ShadowPad: How Attackers hide Backdoor in Software used by Hundreds of Large Companies around the World," Kapersky, August 15 2017. (2) "This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits," Christopher Glyer, Dan Perez, Sarah Jones, Steve Miller, March 25 2020(3)	At first a financially-motivated cybercrime group, APT 41 now also carries out Chinese-sponsored information theft operations. Its first operations date back to 2012. In 2017, the group carried out a supply chain attack named ShadowPad. According to Kapersky it was "one of the largest known supply-chain attacks" (2). In 2018, the group carried out another supply-chain attack dubbed Operation ShadowHammer infecting ASUS Live Update Utility. Though the attack affected more than a million users, according to Kapersky, APT 41 was most interested in specific Asian users. In April 2019, FireEye identified a breach in a publicly-accessible web server at an American research university. Later that year, the group targeted two Hong Kong universities. Throughout 2020, the group carried out a massive cyberespionage campaign, covering a large number of sectors and countries. According to FireEye, the campaign affected 75 of their customers (3). **Level 3**
APT (GhostNet) (aka Snooping Dragon) "GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor, March 29 2009.	The group, likely attributed to the Chinese government, has infected "at least 1,295 computers in 103 countries, of which close to 30% can be considered as high-value diplomatic, political, economic, and military targets" (P.6) according to the report. The report also uncovered the group having breached "computer systems containing sensitive and secret information at the private offices of the Dalai Lama and other Tibetan targets" (P.6). **Level 1**
APT (Goblin Panda) (aka Cycldek, Conimes, 1937CN, Hellsing) "Chinese Hackers Attack Airports Across Vietnam," Tara Seals, July 29 2016. (1) "Cycldek: Bridging the (air) gap," Securelist, June 3 2020. (2)	The group has been active since 2014 and targets mainly defence, energy and government entities in Southeast Asia and specifically Vietnam. They are thought to be Chinese state-sponsored hackers. In 2016, the group compromised the screens, announcement systems and airline systems at airports Vietnam which would display and blare out offensive messages against Vietnam. In 2017, the group used political documents related to Vietnam as bait for a campaign targeted towards large Vietnamese organisations. In 2018, a number of campaigns were recorded against government organisations in Vietnam, Thailand and Laos. **Level 3**
APT 15 (aka Ke3chang, Vixen Panda, GREF, Playful Dragon, Royal APT, Mirage, APT 25, Uncool, Sushi Roll, Tor, BRONZE DAVENPORT, BRONZE PALACE, BRONZE IDLEWOOD, CTG-9246) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020	The group, likely linked to the Chinese state, has targeted various industries in the US, Europe and Africa. In 2010, the group executed Operation Ke3Chang, a cyberespionage campaign against European Ministries of Foreign Affairs ahead of the G20 meeting on Syria. In May 2016, the group launched a campaign against Indian embassy employees worldwide. A year later sensitive information on the UK government and defence technology was stolen from a company contracted by the British government. The last recorded activity was in May 2020. **Level 3**
APT (Lead) (aka TG-3279, Casper) "Detecting threat actors in recent German industrial attacks with Windows Defender ATP," Microsoft, January 25 2017.	The group, possibly linked to the Chinese state, is known for industrial espionage. According to Microsoft, its targets include: multinational, multi-industry companies involved in the manufacture of textiles, chemicals, and electronics, pharmaceutical companies, a company in the chemical industry, a university faculty specialising in aeronautical engineering and research, a company involved in the design and manufacture of motor vehicles, a cybersecurity company focusing on protecting industrial control systems. The group was first discovered in 2016 when Germany-based industrial conglomerate announced that it had been a victim of espionage. **Level 3**

Document	Excerpt
APT 40 (aka Leviathan, TEMP. Periscope, TEMP.Jumper, Bronze Mohawk, Mudcarp, ATK29, Flaccid Rose, Kryptonite Panda, GADOLINIUM, Nanhaishu, Pickleworm) "Leviathan," Mitre Att&ck, April 18 2018. (1) "Leviathan: Espionage actor spear-phishes maritime and defense targets," Proofpoint, October 16 2017. (2) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (3)	According to Mitre Att&ck, APT 40 has been attributed to the "Ministry of State Security's (MSS) Hainan State Security Department and an affiliated front company" (1). It has been active since at least 2013 and executes cyber espionage operations against engineering, transportation, and the defence industry likely in order to advance China's naval force. For example, in 2014, a number of attacks were uncovered against defence contractors, universities with military ties, legal organisations and government bodies, all somehow related to the naval sector. In 2017, the group carried out a spear phishing campaign against a British engineering company and continued to target American entities involved in the naval sector. However, most recently the group seems to have change its focus to target countries with strategic importance in the Road and Belt initiative, notably Cambodia, Belgium, Germany, Hong Kong, Philippines, Malaysia, Norway, Saudi Arabia, Switzerland, the United States, and the United Kingdom. For instance, in 2018, APT 40 targeted individuals in the opposition and organisations in Cambodia involved in the electoral process around the time of the general elections. Moreover, in 2020, Malaysian government-backed organisation denounced an increase in campaigns targeting Malaysian officials. **Level 3**
APT (Lotus Blossom) (aka Spring Dragon, Dragonfish, Elise, ATK1, ST Group, Bronze Elgin, Billbug) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "Thrip: Ambitious Attacks Against High Level Targets Continue," Broadcom, September 9 2019 (2)	Active since at least 2012, the group is likely attributed to the Chinese state. Its main focus is high profile governmental entities, political parties, research universities and the telecommunications sector in countries around the South China Sea. Operation Lotus Blossom (2015-2017) is a long standing cyberespionage campaign that targets Southeast Asian military and governmental organizations. Throughout 2018, the group targeted ASEAN countries in a malware spam campaign and launched operations against military organisations and the maritime communication, satellite communication, media and education sectors. As of 2019, the group was still targeting satellite communication organisations. **Level 1**
APT (Mofang) (aka Superman, BRONZE WALKER) "Mofang: A politically motivated information stealing adversary," Fox It, May 17 2016. (1) "Whitefly: Espionage Group has Singapore in Its Sights," Broadcome, March 6 2019. (2)	The APT Mofang has been active since at least 2012 and is likely sponsored by the Chinese government. The group targets various sectors (government, military, critical infrastructure, and the automotive and weapon industries) in different countries (India, Germany, United States, Canada, Singapore, South Korea) but is known for selecting its targets "based on involvement with investments, or technological advances that could be perceived as a threat to the Chinese sphere of influence" ((1) P.2). For instance, the group targeted a Burmese company with investments in a territory of strategic interest for China's National Petroleum Corporation's investments. In another instance (2018), the group stole information from SingHealth, Singapore's largest public health organisation. The group retrieved sensitive medical information on 1.5 million individuals. **Level 1**
APT 9 (aka Nightshade Panda, APT 9, Group 27, Flowerlady, Flowershow) (potentially freelancers sponsored by the Chinese state) "Advanced Persistent Threat Groups," Mandiant, January 21 2022 (1). "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (2)	According to Mandiant, APT 9 is a freelancer group possibly sponsored by China (1). The group usually targets the health care and pharmaceuticals, construction and engineering, and aerospace and defence sectors in various countries. In May 2015, the group infected visitors of the official President of Myanmar's website ahead of the elections. During the same month, the group also carried out a spear phishing campaign against the US government and a EU media company. Between September and November 2016, the group "compromised two Thai websites to host malware." **Level n/a**
APT 23 (aka Pirate Panda, KeyBoy, Tropic Trooper, BRONZE HOBART) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "It's Parliamentary: KeyBoy and the targeting of the Tibetan Community," Adam Hulcoop, Matt Brooks, Etienne Maynier, John Scott-Railton, and Masashi Crete-Nishihata, November 17 2016. (2)	APT 23, possibly linked to the Chinese state, usually carries out traditional intelligence gathering operations against government and military targets. In 2012, a campaign dubbed Operation Tropic Trooper was uncovered, targeting the Taiwanese government and Philippine's military entities. This campaign continued through 2013-2015, also targeting Hong Kong and the healthcare, transportation, and high-tech industries. In 2016, the group launched an espionage campaign against members of the Tibetan Parliament. In 2020, it was uncovered that the group was targeting officials of the Vietnamese government through spear-phishing emails. **Level n/a**

Document	Excerpt
APT (Platinum) (aka TwoForOne, ATK33) "PLATINUM Targeted attacks in South and Southeast Asia," Microsoft, April 29 2016. (1) "Platinum is back," Securelist, June 5 2019. (2)	The group, active since at least 2009, focuses on information theft. It is possibly linked to China. Its targets are "opportunistic" ((1) P.4); According to Microsoft, "the activity group changes its target profiles and attack geographies based on geopolitical seasons, and may attack institutions all over the world" ((1) P.4). It generally targets governments, diplomatic bodies and telecommunication companies in South and Southeast Asia. For example in 2016, it targeted a legitimate Indian website which offered an email service to its users. It then sent spear phishing emails to the users among which there were government officials. In this way, it attempted to gain control of high-profile target's computers. In 2018, Securelist identified a long standing campaign against diplomatic, government and military entities in South and Southeast Asian countries. **Level n/a**
APT (Rancor) (aka Rancor Group) "Rancor: The Year of The Phish," Check Point, September 22 2019	The group has been active since at least 2017 and is potentially attributable to China. Between 2018 and 2019 APT Rancor was found to be carrying out a 7 month spear-phishing campaign against Southeast Asian government organisations. **Level n/a**
APT (Roaming Tiger) (aka BRONZE WOODLAND, CTG-7273, Rotten Tomato) "BBSRAT Attacks Targeting Russian Organizations Linked to Roaming Tiger," Bryan Lee and Josh Grunzweig, December 22 2015.	Roaming Tiger is possibly state-sponsored by China and active since at least 2014. It targets high-profile Russian targets and Russian speaking nations. In August 2015, Paloalto uncovered attacks exploiting a Microsoft Office vulnerability to take control of the victim's computer. **Level n/a**
APT (Shadow Network) "SHADOWS IN THE CLOUD: Investigating Cyber Espionage 2.0," Information Warfare Monitor, April 6 2010.	According to Citizen Lab, Shadow Network is a "complex ecosystem of cyber espionage that systematically compromised government, business, academic, and other computer network systems in India, the Offices of the Dalai Lama, the United Nations, and several other countries," (P.4) likely linked to the PCR. The group steals highly sensitive information, for instance encrypted documents suspected to be from the Indian government or letters sent from the Dalai Lama's office in 2009. **Level n/a**
APT (Scarlet Mimic) "Scarlet Mimic: Years-Long Espionage Campaign Targets Minority Activists," Robert Falcone and Jen Miller-Osborn, January 24 2016.	The group is known for targeting minority right groups and those sympathetic to them, notably Uyghur and Tibetan activists as well as a Turkic Muslim minority residing primarily in northwest China. The targets seem to align with Chinese interests and the group's IP also overlaps with that of Putter Panda and APT 2. Therefore, the group could possibly be linked to the PRC. The latest recorded operation was an information gathering campaign against Indian and Russian organisations that track activist and terrorist activities in their respective countries. The group had a specific interest in Muslim activists and activists critical of Putin. **Level n/a**
APT (Gallium) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	APT Gallium was first uncovered by Microsoft in 2018. It is possibly linked to China and carries out espionage operations against the telecommunications sector. Although it remains active, its activity has gone in decrease since 2019. **Level n/a**
APT (Operation Shady RAT) "Revealed: Operation Shady RAT," McAfee, March 2011.	The group, active since at least 2006, is thought to be sponsored by China. The group has targeted multiple sectors in multiple countries. The McAfee report lists some of its operations: "In 2006 (...) we saw only eight intrusions: two on South Korean steel and construction companies, and one each on a South Korean Government agency, a Department of Energy Research Laboratory, a U.S. real-estate firm, international trade organizations of an Asian and Western nations and the ASEAN Secretariat" (P.6) (...) "In 2007, the pace of activity jumped by a whopping 260 percent to a total of 29 victim organizations(...) four U.S. defense contractors, Vietnam's government-owned technology company, US federal government agency, several U.S. state and county governments, and one computer network security company. The compromises of the Olympic Committees of two nations in Asia and one Western nation began that year as well. In 2008, the count went up further to 36 victims, including the United Nations and the World Anti-Doping Agency, and to 38 in 2009. Then the number of intrusions fell to 17 in 2010 and to 9 in 2011, likely due to the widespread availability of the countermeasures for the specific intrusion indicators used by this specific actor" (P.6). **Level n/a**

Document	Excerpt
APT (PKPlug) (aka HenBox, Farseer) "PKPLUG: Chinese Cyber Espionage Group Attacking Southeast Asia," Alex Hinchliffe, October 3 2018.	The group is known for targeting Myanmar, Taiwan, Vietnam, and Indonesia; and likely also in various other areas in Asia, such as Tibet, Xinjiang, and Mongolia. The targets align with the PCR's interests thus, it is possible that PKPlug is state-sponsored. Most of the countries are part of ASEAN, are involved the Belt and Road Initiative and/or have some involvement in the South China Sea issue, both strategically important to China. In November 2013, Blue Coats Lab uncovered an attack against Mongolian or Mongolian-related targets. In 2016 activity was reported against Myanmar in two instances: one using ASEAN issues as bait and another using information on Myanmar activists. In 2017, spear-phishing against Japan and Myanmar were recorded. In 2018, Unit 42 discovered a campaign that used a malicious Android app to target Uyghurs and a minority Turkic group living in Northwest China. The latest recorded activity in February 2019 employed decoy documents on Myanmar political news for the attack. **Level n/a**
APT (SabPub) "SabPub Mac OS X Backdoor: Java Exploits, Targeted Attacks and Possible APT link," Securelist, April 12 2014.	On the attacks, Securelist reports: "This new threat is a custom OS X backdoor, which appears to have been designed for use in targeted attacks. After it is activated on an infected system, it connects to a remote website ... to fetch instructions. The backdoor contains functionality to make screenshots of the user's current session and execute commands on the infected machine." "Several reports exist which suggest the attack was launched through e-mails containing an URL pointing to two websites hosting the exploit, located in US and Germany. The timing of the discovery of this backdoor is interesting because in March, several reports pointed to Pro-Tibetan targeted attacks against Mac OS X users. The malware does not appear to be similar to the one used in these attacks, though it is possible that it was part of the same or other similar campaigns." Because the attacks align with Chinese interests, it is possible that the group is state-sponsored. **Level n/a**
APT (BRONZE DUDLEY) (aka Vicious Panda) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	A campaign by BRONZE DUDLEY in 2020 employing information on Covid19 to attack the Mongolian public sector uncovered past operations carried out by the same APT. In 2015, the group utilised phishing emails and infected legitimate-looking documents against the offices of the Mongolian government. In 2017, another similar campaign was carried out but this time against Belarussian government entities. Because the attacks align with Chinese interests, it is possible that the group is state-sponsored. **Level n/a**
APT (BlackTech) (aka CIRCUIT PANDA, Temp.Overboard, HUAPI, Palmerworm, T-APT-03) "Waterbear Returns, Uses API Hooking to Evade Security," Vickie Su, Anita Hsieh, Dove Chiu, December 11 2019 (1) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (2)	Black tech is a cyberespionage group thought to be linked to the Chinese state. Its targets are countries in East Asia, especially Taiwan and to a lesser extent Japan and Hong Kong. For example, Operation PLEAD in 2012 targeted Taiwanese government bodies and private entities. In 2018, the group employed stolen digital certificates to launch a malware attack against Taiwanese security company Changing Information Technology Inc. Most recently, in 2019, a APAC-based security vendor was also targeted by BlackTech. **Level n/a**

Colombia

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber (2021):	Comando Conjunto Cibernetico
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	46.75 (74th)
Internet Penetration (2020)	70%
Internet Freedom Score	65/100 (Partly free)

Transparency Description

Colombia's scores for the declared and perceived capability rating differ slightly. Colombia has overtly stated its aspirations to develop offensive cyber capabilities. In 2021, Colombia established the Joint Cyber Command whose mandate is to develop military operations in cyberspace to defend sovereignty. However, no information regarding current structure, capability, and core principles has been disclosed. At the aspirational level, the Ministry of Defence declared in 2016 that the armed forces ought to take steps to disrupt, deny, degrade or destroy potential adversary's systems. In an interview released in 2018, officials from the Ministry of Defence stated that the Department of Communications and Cyber Defence is committed to strengthening both defensive and offensive cyber capabilities. No offensive cyber operation has been attributed to Colombia to this date.

Declared Capability Rating

Score ■■■□□

Stated aspiration for offensive cyber capabilities. Colombian strategies and officials have made references to the need to develop offensive cyber capabilities in order to strike back against malicious actors. While there is a Joint Cyber Command, it remains unclear to what extent their capability is aspirational or already developed and integrated within their overall military structure.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"Cyber Joint Command: Military Operations in Cyberspace," Joint Cyber Command Colombia, 2021.	Describes Colombia's Joint Cyber Command in charge of «developing military operations in cyberspace to defend sovereignty » Level 3
"La ciberdefensa en Colombia, el nuevo frente de la guerra," Semana, July 14 2018.	In an interview with Colombian military officials, the Army's Cede-6 Department of Communications and Cyber Defence is described as being "committed to strengthening the entity's defensive and offensive capabilities, especially with the GETDE (Army Digital Transformers Group)." [Original: el Departamento de Comunicaciones y Ciberdefensa Cede-6 del Ejército apuesta por el fortalecimiento de las capacidades defensivas y ofensivas de la entidad, especialmente con el GETDE (Grupo de Transformadores Digitales del Ejército)]. The article also alludes to the development of in-house software and notes there are five confidential software projects as of 2018: "This digital transformation not only eliminates the need to acquire software from private enterprise, but is currently developing five classified software projects." [Original: Esta transformación digital no solo elimina la necesidad de adquirir servicios tecnológicos de la empresa privada, sino que actualmente tiene cinco proyectos de software clasificados.] Level 1

Document	Excerpt
"Documento Conpes 3854," Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional, Dirección Nacional de Inteligencia, Departamento Nacional de Planeación, April 11 2016.	No official indications of Offensive Cyber Capability. **Level 0**
"Vision de Futuro de Las Fuerzas Armadas," Ministerio de Defensa Nacional, 2016.	In the vision document for the Armed forces, the Ministry of Defence states that their forces "must also take steps and actions to disrupt, deny, degrade or destroy the information handled by the information and communications systems of the potential adversary. In this way, the Public Force will be able to neutralise the enemy attack, obtain superiority in cyberspace to have the freedom to defend strategic objectives, obtain adequate levels of security for its own systems and minimise the possible effects of an attack." **Level 1**
"Documento Conpes 3701," National Council for Economic and Social Policy Republic of Colombia, July 14 2011.	No official indications of Offensive Cyber Capability **Level 0**

Perceived Capability Rating

Score ■■□□□

Perceived to be working on obtaining offensive cyber capabilities. No public information was found on past Colombian cyber operations that go beyond spyware acquired from foreign vendors.

Data availability rating (1 being highest number of sources, 21 lowest): **18/21**

Document	Excerpt
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The document lists Colombia as one state "considered possessing substantial military cyberspace capabilities and some of these countries have announced intentions to create cyber commands and/or cyberattack capabilities," (P. 188). **Level 2**
"Deconstructing cyber security in brazil: Threats and Responses," Gustavo Diniz, Robert Muggah and Misha Glenny, December 2014.	Notes that Brazil and Colombia are the only South American countries to encourage the armed forces to take a large role in cyber threats (P. 23). **Level 2**
"Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014.	In one instance, Colombia was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, 2011.	This 2011 document notes that the Colombian Ministry of Defence intends to develop the ability to conduct cyberattacks against aggressors (P. 16). **Level 2**

Croatia

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber (2021):	Cyber Command (ZzKP)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	83.12 (15th)
Internet Penetration (2020)	78%
Internet Freedom Score	n/a

Transparency Description

Croatia's scores for the declared and perceived capability rating only differ slightly at the lower-end of the spectrum. It has overtly stated its aspirations to develop offensive cyber capabilities. In 2019, the Ministry of Defence sought to establish a Cyber Command (*Zapovjedništvo za kibernetički prostor*) with the aim to defend the government's networks and system, as well as to offer emergency civilian protection. In 2021, the website of the Croatian Armed Forces specified that one of the main tasks of the Cyber Command is to develop capabilities to carry out operations in cyberspace. However, no information regarding existing offensive cyber capabilities, structure and core principles has ever been disclosed. No aspirations to obtain offensive cyber capabilities are perceived by outside sources.

Declared Capability Rating

Score

Stated aspiration for offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **7/10**

Document	Excerpt
"Cyberspace Command (ZzKP)," Official Website Croatian Armed Forces, September 14 2021.	The website describes the development of "capabilities to carry out operations in cyberspace" as one of the main tasks of the Command. [Original: razvija sposobnosti za provedbu operacija u kibernetičkom prostoru] Level 1
"Croatia is equipping itself for the fourth dimension of warfare," VL, February 21, 2019.	The Croatian Armed Forces sought to establish its Cyber Command by the summer of 2019. Its primary goal is to defend MoD networks and systems, and to offer emergency civilian protection if need be. It has reportedly participated in NATO exercises, but no reference to offensive capabilities is made. Level 0
"National Security Strategy of the Republic of Croatia," Republic of Croatia, July 14 2017.	"The Armed Forces of the Republic of Croatia are developing the capabilities of conducting combat operations in defence of their own territory on land, sea and air and in cyberspace, independently and in cooperation with allies, until the activation of the collective defense." (P.11) [Original: Oružane snage Republike Hrvatske razvijaju sposobnosti provedbe borbenih operacija u obrani vlastitog teritorija na kopnu, moru i zraku te u kibernetičkom prostoru, samostalno i u suradnji sa saveznicima, do aktiviranja mehanizma kolektivne obrane.] Level 0
"The National Cyber Security of The Republic of Croatia," Republic of Croatia, October 7, 2015.	No Official Indications of Offensive Cyber Capability Level 0

Perceived Capability Rating

Score

No aspirations to obtain offensive cyber capabilities were perceived.

Data availability rating (1 being highest number of sources, 21 lowest): **21/21**

Czech Republic

Cyber Transparency Score Transparent and Low Capability

Declared Capability Rating ■■□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber (2019):	Cyber Forces Command
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	92.21 (4th)
Internet Penetration (2020)	81%
Internet Freedom Score	n/a

Transparency Description

The Czech Republic's scores for the declared and perceived capability rating are identical at the lower-end of the spectrum. It appears to have the aspiration to develop offensive cyber capabilities. While all official documents largely focus on defensive capabilities and resilience, the 2016 Cyber Security Strategy already stated that one of Czech Republic main goals is to train experts specialised, *inter alia*, in offensive approach to cyber security. The 2018 Cyber Defence Strategy further provided that, besides cyber defence, the National Cyber Operations Centre (NCOC) will have to develop its capabilities to support military operations. While no sources reported on past cyber operations, the Czech Republic is externally perceived as working on obtaining offensive cyber capabilities. According to media reports, a Cyber Force Command has been established in Brno in 2019, and is expected to become fully operational by 2025. No offensive cyber operations have been attributed to the Czech Republic.

Declared Capability Rating

Score ■■□□□

Sanctioned media reporting on offensive cyber details and/or operations by an official (capabilities likely to exist but unconfirmed by official resources, the extent of which being unknown). Several government documents mention the aspirations to develop offensive capabilities and the re-organization of military cyber and information operations. The established Cyber Forces Command appears to largely focus on carrying out information and psychological operations to support military operations at the tactical level.

Data availability rating (1 being highest number of sources, 10 lowest): **5/10**

Document	Excerpt
"VOJENSKÉ ZPRAVODAJSTVÍ ZAJIŠŤUJE KYBERNETICKOU OBRANU ČESKÉ REPUBLIKY," Military Intelligence, 2021.	The document highlights the need for Czech military to develop their defensive cyber capabilities. Nonetheless, it makes no mention of offensive capabilities. Level 0
"Kybernetické armádní síly podpořili specialisté z Olomouce," ITBiz, September 1, 2020.	"According to Jana Gallová, spokeswoman for the 103rd CIMIC / PSYOPS Center, the task of the cyber forces is primarily the protection of information technology networks and military weapon systems, the support of strategic communications and the acquisition and provision of information from the information environment and the cyber world. ... They work closely with military intelligence to protect cyberspace and conduct military cyber operations." Level 2

Document	Excerpt
"Cyber Forces Command," Ministry of Defence and Armed Forces of the Czech Republic, February 7, 2020.	"Cyber Forces Command: On tactical level, they monitor, plan and control operations in cybernetic and informational domain, including the support of STRATCOM of the Army of the Czech Republic. CIW forces provide the ability to defend domestic parts of cyberspace, conduct InfoOps, InfoOps in cyberspace, PsyOps and CMI/CIMIC. Within the cyberspace defence, they closely cooperate with Military Intelligence, and their individual capabilities complement each other." **Level 2**
"Cyber Defence Strategy of the Czech Republic 2018-2022", National Cyber Operations Centre, 2018	While the strategy does not make explicit references to offensive cyber capabilities of government, it notes that "Besides cyber defence of the Czech Republic, NCOC will have to develop its capabilities to support military operations. They will cover operational up to tactical levels and will include both combat support in other spheres and operations carried out exclusively in cyberspace." Furthermore, the strategy also encourages the development of a cyber deterrence strategy that includes a punishment capability. **Level 1**
"Zajištění požadovaných schopností kybernetické obrany," Miroslav Feix and Dalibor Procházka, April 2017.	The document makes recommendations about what the Czech Republic should develop, including offensive capabilities, suggesting they do not have them yet. The author, Miroslav Feix, is the Commander of the Czech Cyber Command. **Level 1**
"National Cyber Security Strategy of the Czech Republic for the Period from 2015 to 2020," NCKB, 2016.	One of the (numerous) main goals is to "...train experts specialised in questions of active counter-measures in cyber security and cyber defence and in offensive approach to cyber security in general." (P. 18). **Level 1**

Perceived Capability Rating

Score ■■□□□

Perceived to be working on obtaining offensive cyber capabilities. Almost no reports were found on past cyber operations or the state of the Czech offensive cyber programme, which largely remains aspirational until the Cyber Command becomes fully operational in 2025.

Data availability rating (1 being highest number of sources, 21 lowest): **21/21**

Document	Excerpt
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	"...according to media reports, the Czech Republic opened cyber command in Brno in January 2019 with initial operational capability planned as of 2020 and full operational capability as of 2025..."(P. 187) **Level 2**

Democratic People's Republic of Korea (DPRK)

Cyber Transparency Score Very Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■■■

Organization for Offensive Cyber (2021):	Bureau 121 of the Reconnaissance General Bureau and the KPA (unconfirmed)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	n/a
Internet Penetration (2013)	0.00 %
Internet Freedom Score	n/a

Transparency Description

A complete lack of transparency is observed for the Democratic People's Republic of Korea. Given its closed-off nature, the North Korean government has not officially disclosed that it has offensive cyber capabilities nor has it released any official cyber strategy or doctrine. However, North Korea is largely perceived to having launched several successful offensive cyber operations. A high level of open-source findings confirms that North Korean offensive cyber capabilities are fully integrated within the military, especially by Bureau 121 of the Reconnaissance General Bureau (RGB) and by the army (KPA). It is broadly acknowledged that established North Korean capabilities are able to effectively degrade and destroy systems and infrastructures of adversaries. Several states and public reports have overtly attributed relevant APTs (such as Covellite, Kimsuky, Lazarus Group, Hidden Kobra, etc.) to North Korea or to state-sponsored North Korean Groups. Several cyberattacks have been attributed to North Korea and several North Korean hackers have been indicted.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of a declared offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■☐☐☐

Viewed as having launched several successful offensive cyber operations, with the proven capability to denigrate and destroy enemy systems or infrastructure. The DPRK is widely believed to have obtained, integrated and used relatively unsophisticated offensive cyber capabilities to achieve asymmetric advantages over adversaries, for the purpose of financial gain (cybercrime) or as a coercive response to foreign pressure (cyber sabotage).

Data availability rating (1 being highest number of sources, 21 lowest): **4/21**

Document	Excerpt
Cyber-related sanctions "Sanctions by the Numbers: Spotlight on Cyber Sanctions," Jason Bartlett and Megan Ophel, May 4 2021. (1) "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," US Department of the Treasury, September 13 2019. (2)	Since 2012, the US Treasury Department has issued more than 15 cyber-related sanctions against North Korean individuals and entities, oftentimes linked to branches of the DPRK's government. For example, the US sanctioned three North-Korea state-sponsored malicious groups, *Lazarus*, *Bluenoroff*, and *Andariel* for their role in the Sony Hack, in the WannaCry ransomware and other financial-related cyberattacks Level 5

Document	Excerpt
Cyber-related sanctions "Sanctions by the Numbers: Spotlight on Cyber Sanctions," Jason Bartlett and Megan Ophel, May 4 2021. (1) "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," US Department of the Treasury, September 13 2019. (2)	Since 2012, the US Treasury Department has issued more than 15 cyber-related sanctions against North Korean individuals and entities, oftentimes linked to branches of the DPRK's government. For example, the US sanctioned three North-Korea state-sponsored malicious groups, *Lazarus*, *Bluenoroff*, and *Andariel* for their role in the Sony Hack, in the WannaCry ransomware and other financial-related cyberattacks **Level 5**
"Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," US Department of Justice, February 17 2021.	In 2021, the US Department of Justice indicted three North Korea military hackers for their scheme to commit financial and cyberattacks globally. This indictment expands the 2018 one "by adding two new defendants and recent global schemes to steal money and cryptocurrency from banks and businesses". According to the press release, two defendants were members of the DPRK's military intelligence agency, the Reconnaissance General Bureau" **Level 4**
"Cyber Operations Tracker," Council on Foreign Relations, 2020.	Identifies 29 cyberattacks sponsored by North Korea. **Level 4**
"COUNCIL IMPLEMENTING REGULATION (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Official Journal of the European Union, July 30 2020. (1) "Consolidated List of Financial Sanctions Targets in the UK," Office of Financial Sanctions Implementation HM Treasury, December 31 2020. (2)	In 2020, the European Union imposed sanctions on one North Korean entity for its role in the WannaCry cyberattack. The company, Chosun Expo, was found to be linked to APT38, also known as Lazarus Group. After Brexit, the UK implemented the sanctions against the same individuals and entities targeted by the EU. **Level 4**
"Israel says it fended off North Korean hack attempt against defense industry," The Times of Israel, August 12 2020.	Israeli attribution of 2020 cyberattack against its defence industry to North Korea: "The Defence Ministry said hackers from a group linked to the North Korean government targeted Israeli defence officials, luring them with fake job offers in a failed attempt to gain access to the databases of the country's top defence industries. In a statement, the ministry said the attempted cyber-attack by the Lazarus Group was thwarted and no sensitive information was compromised." **Level 3**
"FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks," Cybersecurity and Infrastructure Security Agency, August 26 2020.	US attribution of 2020 ATM-scheme to North Korea: "Working with U.S. government partners, CISA, Treasury, FBI, and USCYBERCOM identified malware and indicators of compromise (IOCs) used by the North Korean government in an automated teller machine (ATM) cash-out scheme—referred to by the U.S. Government as "FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks."" **Level 3**
"North Korean Advanced Persistent Threat Focus: Kimsuky," Cybersecurity and Infrastructure Security Agency, October 27 2020.	US attribution of 2020 cyber espionage campaign to North Korean APT, acting on behalf of the DPRK government: "This advisory describes the tactics, techniques, and procedures (TTPs) used by North Korean advanced persistent threat (APT) group Kimsuky – against worldwide targets – to gain intelligence on various topics of interest to the North Korean government. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA." **Level 1**
"Guidance on the North Korean Cyber Threat," Cybersecurity and Infrastructure Agency, April 15 2020.	"DPRK state-sponsored cyber actors primarily consist of hackers, cryptologists, and software developers who conduct espionage, cyber-enabled theft targeting financial institutions and digital currency exchanges, and politically-motivated operations against foreign media companies." (P. 2). It usually does so to raise revenue for the regime. **Level 3**
APT (Covellite) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	APT (Covellite), likely linked to the DPRK, is known for attacking civilian electric energy sectors around the globe. The primary victims are Europe, East Asia and the US. Covellite toolkit and infrastructure bears similarities to the Lazarus Group but the relation between them is unsure. Experts categorize Covellite as a capable and dangerous threat to the ICS sector. **Level 4**

Document	Excerpt
APT (Kimsuky) (aka Velvet Chollima) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Operation Kabar Cobra," AhnLab Security Emergency-response Center (ASEC), February 28 2019. (2) "Kimsuky Organization, Operation Stealth Power Silent Operation," 이스트시큐리티 알약 블로그, April 3 2019. (3) "Analysis of the APT Campaign 'Smoke Screen' targeting to Korea and US," EST Security, April 17 2019. (4) "ASEC Report, Vol.93," AhnLab, October 10 2019. (5)	The group is known for carrying out cyberespionage operations against South Korean targets and is attributed to South Kora. In 2014, the South Korean government accused North Korea of information theft attacks against the Korea Hydro and Nuclear Power (KHNP) which controls South Korea's 23 nuclear reactors. According to the government only non-critical networks were affected. In 2019, the group carried out multiple operations: Operation "Kabar Cobra" a cyberespionage campaign against the South Korean media, defence-related entities and cryptocurrency companies ; "Stealth Power," a spear-phishing attack against South Korean employees working in the diplomacy, security, reunification sectors and in issues related to North Korea; "Smoke Screen," and "Red Salt", both an extension of Operation Stealth Power. Most recently, the group employed documents with Covid19 content to inject malware (2020). Because the targets align with North Korea's interests, it is possible that the group is state-sponsored. **Level 3**
APT-C-26 (aka Lazarus Group, Hidden Cobra, Labyrinth Chollima, Group 77, Hastati Group, Whois Hacking Team, NewRomanic Cyber Army Team, Zinc, Nickel Academy, , Bureau 121, ATK3, APT 38, APT 37, APT-C-26, T-APT-15, SectorA01) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "The Hack of Sony Pictures: What We Know and What You Need to Know," Trend Micro, December 8 2014. (2) "Lazarus: History of mysterious group behind infamous cyber attacks," Symantec, May 25 2017. (3)	The group, attributed to the DPRK and operational since 2009, became well known in 2013 after a number of attacks paralysing the systems of South Korean broadcasters and a financial institution. In 2014, Operation Blockbusters was uncovered: a large breach on the Sony corporate network which was attributed to this group. As a consequence of the attack, documents containing data and information on Sony's employees and senior executives were leaked to the public and Sony had to temporarily shut down its network. In 2015, a number of espionage attacks against South Korean manufacturing companies were attributed to the group. In 2016, the Lazarus Group targeted Bangladesh Central Bank in a SWIFT attack, stealing 81 million dollars. Later, in 2017, the WannaCry ransomware attack was attributed to the group. This was a widespread campaign that gained media attention for having compromised at least 200,000 systems in over 100 countries and having caused the networks of many large organizations around the world, (i.e. the NHS in the UK) to go temporarily offline. Western intelligence agencies attributed WannaCry attacks to North Korea, followed shortly by a US indictment for the Sony and WannaCry attacks. Since then, the APT has targeted "87 organisations in many different sectors (majority Government and Defence) across the globe, predominantly in the United States" ((1) P. 175) and attacked South Korean Cryptocurrency businesses. In 2019, the group was found to be also targeting an Israeli defence company. In September of the same year, two affected European companies recorded "attacks against aerospace and military companies in Europe and the Middle East" ((1) P. 176) **Level 5**
APT 37 (aka Reaper, Ricochet Chollima, Group 123, Red Eyes, Venus 121, ATK4, Operation Daybreak, Operation Erebus, ScarCruft) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "APT37 (REAPER): The Overlooked North Korean Actor," FireEye, February 20 2018. (2) "Dragon Messenger," ESTsecurity Security Response Center, August 23 2019. (3) "The 'Spy Cloud' Operation: Geumseong121 group carries out the APT attack disguising the evidence of North Korean defection," ESTsecurity Security Response Center, March 2020. (4)	This group is also thought to be linked to the Lazarus Group. It targets primarily South Korea and to a lower degree Japan, Vietnam and the Middle East. The compromised sectors are usually in chemicals, electronics, manufacturing, aerospace, automotive, and healthcare. Between 2014 and 2017 "APT37 targeting concentrated primarily on the South Korean government, military, defence industrial base, and media sector" ((2) P. 5). In 2017, "APT37 targeted a Middle Eastern company that entered into a joint venture with the North Korean government to provide telecommunications service to the country... At that time, other targets included individuals involved in international affairs and trade issues, the general director of a Vietnamese international trading and transport company, and possibly individuals working with Olympics organisations assisting in securing resources for athletes" ((2) P. 6). Its most recent attacks are Operation "Dragon messenger" distributing malware through a malicious app "disguised as a fundraising service for supporting North Korean defectors" ((3) P. 1) in 2019 and Operation "Spy Cloud" in 2020, a spear phishing attack against users in South Korea. **Level 4**
APT (Wassonite) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Confirmed: North Korean malware found on Indian nuclear plant's network," Catalin Cimpanu, October 30 2019. (2)	The group was first discovered after an attack on an Indian nuclear plant in October 2019. India is their main target and possibly South Korea and Japan. Because the targets align with North Korea's strategic interests, it is possible that the group is state-sponsored. **Level 4**
"Panel report UN Security Council," March 5 2019. (primary source) (1) "UN report links North Korean hackers to theft of $571 million from cryptocurrency exchanges," Sean Lyngaas, March 12 2019. (secondary source) (2)	The UN attributes the 2019 financial cyberattacks to North Korea: according to CyberScoop "North Korean government-sponsored cyberattacks on financial institutions to illegally transfer funds "have become an important tool in the evasion of sanctions and have grown in sophistication and scale since 2016," says the U.N. panel report". **Level 3**

Document	Excerpt
"The All-Purpose Sword: North Korea's Cyber Operations and Strategies," Kong Ji Young, Lim Jong In, Kim Kyoung Gon, 2019.	The document mentions several prominent cyberattacks attributed to North Korea dating back to 2013, including Campaign Kimsuky and Operation KHNP (both espionage); Operation DarkSeoul and Operation BlockBuster; and the Bangladesh Central Bank Heist and WannaCry. (P. 7). **Level 4**
"Worldwide Threat Assessment of the US Intelligence Community," Daniel R. Coats, January 29 2019.	"North Korea poses a significant cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyberattacks. North Korea continues to use cyber capabilities to steal from financial institutions to generate revenue." (P. 6). **Level 3**
"North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," US Department of Justice, September 6 2018.	In 2018, the US Department of Justice indicted a North Korean national, Park Jin Hyok, "for his involvement in a conspiracy to conduct multiple destructive cyberattacks around the world resulting in damage to massive amounts of computer hardware, and the extensive loss of data, money and other resources". According to the complaint, "Park was a member of a government-sponsored hacking team known to the private sector as the "Lazarus Group", and worked for a North Korean government front company, Chosun Expo Joint Venture, to support the DPRK government's malicious cyber actions". This includes his role in the Sony Pictures hack, the Bangladesh Bank cyber heist, and the WannaCry ransomware. **Level 4**
"It's Official: North Korea Is Behind WannaCry," Thomas P. Bossert, December 18 2017. (1) "Foreign Office Minister condemns North Korean actor for WannaCry attacks," UK Government, December 19 2017. (2)	US and UK attribute the 2017 WannaCry ransomware to Lazarus group: the US declaration was made by Trump aide Thomas Bossert to the Wall Street Journal. At the same time, the UK government released a statement supporting the attribution. **Level 4**
"Military and Security Developments Involving the Democratic People's Republic of Korea," Report to Congress, December 15 2017.	In a report to the US Congress the office of the Secretary of Defence states that "North Korea uses offensive cyberoperations as a cost-effective and deniable asymmetric tool to carry out regime goals on a global scale." (P.1) **Level 4**
"Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities," Committee on Armed Services, United States House of Representatives, One Hundred Fifteenth Congress, First Session, March 1 2017.	Observes "North Korea is starving, both in the literal sense of being poor as well as feeling starved of attention. Cyber capabilities, such that used against Sony Motion Pictures, is a way for the North Koreans to actualize their tantrums as well as have a direct, though limited, impact in South Korea and United States. North Korea knows it cannot keep pace with American and South Korean military capabilities, so cyber sabotage offers unique benefits, as does cybercrime to raise hard currency. Even so, their behavior often closely matches the overall diplomatic environment. Whenever Pyongyang walks away from Panmunjom or has fresh sanctions slapped on it, expect a cyber outburst." **Level 4**
"2016 Defence White Paper," Ministry of National Defence Republic of Korea, December 31 2016.	Identifies North Korea as the cause of the 2014 Sony pictures hack (a consensus that is widely shared amongst the international community) (P. 10). States: "Notably, North Korea has developed a 6,800-strong unit of trained cyberwarfare specialists who are launching various forms of cyber-attacks." (P. 27). **Level 4**
"North Korea suspected of hacking Seoul's subway operator last year," The Straits Times, October 5 2015.	South Korean attribution of 2015 Seoul Subway cyberattack to DPRK: A Vice article reports that "A South Korean legislator revealed this week that a report from the nation's intelligence service suggested that the North Korean government might have been behind a hack of the Seoul Metro system" **Level 3**
"South Korea blames North Korea for December hack on nuclear operator," Ju-min Park and Meeyoung Cho, March 17 2015.	South Korean attribution of 2014 Korea Hydro and Nuclear Power cyberattacks to North Korea: according to a statement from the Seoul central prosecutors' office "The malicious codes used for the nuclear operator hacking were the same in composition and working methods as the so-called 'Kimsuky' that North Korean hackers use" **Level 4**
"North Korea's Cyber Operations," CSIS, December 2015.	North Korea is believed to have developed offensive cyber capabilities that it employs in military operations. **Level 4**

Document	Excerpt
"Here's The Full FBI Statement Calling Out North Korea For The Sony Hack," Michael B Kelley, December 19 2014.	US attribution of 2014 Sony Hack to North Korea: "As a result of our investigation, and in close collaboration with other U.S. Government departments and agencies, the FBI now has enough information to conclude that the North Korean government is responsible for these actions." **Level 4**
"Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses," Nir Kshetri, July 22 2014.	"In 2009, then-leader Kim Jong Il was reported to order the cyber command unit to expand to 3,000 hackers. Currently, the Unit is estimated to have 3,000–4,000 personnel engaged in cyber warfare". "According to a South Korean security official, North Korea also has about 12,000 highly skilled civilian hackers". Also, interestingly, "An estimated 1,000 North Korean hackers are believed to be in undercover assignments working for educational software companies, animation companies and other firms in China, Southeast Asia, and Europe," (P. 189-190). **Level 4**
"North Korea 'behind South Korean bank cyber hack'," BBC News, 3 May 2011.	South Korean attribution of 2011 Nonghyup Bank attack to DPRK: "The Seoul prosecutors' office called it "unprecedented cyber-terror deliberately planned" by North Korea." **Level 4**

Denmark

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber):	Danish Defense (unconfirmed)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	84.42 (13th)
Internet Penetration (2020)	97%
Internet Freedom Score	n/a

Transparency Description

Denmark's declared capability ranks higher than externally perceived estimates of its offensive capability. It has been transparent over the years about its ability to carry out offensive cyber capabilities, and has also officially declared its will to contribute to NATO by means of cyber weapons. In 2012, the Ministry of Defence overtly described the Danish military capability as encompassing both defensive and offensive military operations in cyberspace. Denmark has published a Military Doctrine for Cyberspace Operations which offers a detailed insight into the taxonomy of offensive cyber effects, order of battle, conditions of employment, as well as the core operational principles for conducting offensive operations. Offensive cyber operations (as well as defensive) are conducted by the CNO Capacity and the performing entity is the Centre for Cyber Security (CFCS). However, limited details regarding the structure of the unit have been released. Its externally perceived capabilities rank lower, with past operations reportedly limited to intelligence and defensive operations.

Declared Capability Rating

Score

Denmark is not only transparent about its ability to carry out offensive cyber capabilities, but its published doctrine shows how these capabilities are integrated within its overall command structure and operations.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"Cyber Security - Denmark rearms in the fights against digital threats," Danish Ministry of Defence (last updated October 27, 2020)	"Since 2016, Denmark has contributed to NATO's defence in cyber space and is now preparing also to be able to contribute to NATO by means of effects from the offensive part of the capacity. Thus, by means of cyber weapons Denmark can deliver an effect against a target in a NATO area of operations. In connection with the use of the offensive cyber capacity in an international operation the capacity will be subordinated to the Chief of Defence like any other military capacity. The Danish military capacity for operations in cyber space is still under construction and is expected to be fully operative in 2019." Level 3
"Joint Doctrine for Military Cyberspace Operations", Royal Danish Defence College, September 2019	The Danish Joint Doctrine offers a detailed insight into its taxonomy of offensive cyber effects, general order of battle, conditions of employment, and the principles of operation. It offers limited details offensive cyber command structure. Level 4.5
"Danish Defence Agreement 2013-2017," Danish Ministry of Defence, November 30 2012.	The agreement establishes the Danish military capacity "to carry out defensive and offensive military operations in cyberspace". Level 3

Perceived Capability Rating

Score 

Perceived to be working on obtaining offensive cyber capabilities. Past operations are limited to an intelligence operation, conducted in cooperation with the US NSA against neighbouringg countries. As a result, the rating remain relatively low.

Data availability rating (1 being highest number of sources, 21 lowest): **15/21**

Document	Excerpt
"The Defence Intelligence Service let the United States spy on Angela Merkel, French, Norwegian and Swedish top politicians through Danish internet cables", DR, May 30, 2021	The Danish foreign intelligence agency co-operated with the US NSA to tap Danish internet cables to spy on foreign heads of state and other high-ranking officials, including from Germany Sweden, Norway and France, through the Xkeyscore tool made available by the NSA. **Level 2**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The book alleges Denmark allocates 9 million Euros per year for their cyber command (P. 194). **Level 2**
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	The paper discusses NATO's changing stance, which is now more and more invested in offensive cyber missions. It also mentions that 5 NATO members have announced that they would contribute national cyber forces to NATO missions and operations. This group includes Denmark. (P. 2). A table also lists Denmark as having launched a Military Cyber Operation (MCO), and lists its growth as 'present'. (P. 7). **Level 3**
"Defining offensive cyber capabilities," Tom Uren, Bart Hogeveen and Fergus Hanson, July 4 2018.	Notes that "...some smaller nations, such as the Netherlands, Denmark, Sweden and Greece, are also relatively transparent about the fact that they have offensive cyber capabilities." **Level 2**
"Denmark To Develop Offensive Cyber Capability," DefenseNews, January 8 2015.	"Denmark has responded to a series of cyberattacks against private and state defence organizations by establishing an Offensive Cyber Warfare (OCW) unit to repel assaults and launch counter-strikes." **Level 2**
Denmark is ready for cyber attacks, Politeken, January 1, 2015	Following a serious breach of a Danish arms maker in 2014, the the Danish government allocated up to DKK 465m ($73.6m) from 2015 to 2017 to ensure the Defence Intelligence Services (FE) are capable of launching cyberattacks this year, a move away from its current focus on defence only. **Level 2**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	As noted in 2011, "The Defence Intelligence Service is responsible for finding and countering cyber threats and is planning to establish a cyberwarfare unit." (P. 18) **Level 2**

Ecuador

Cyber Transparency Score Untransparent

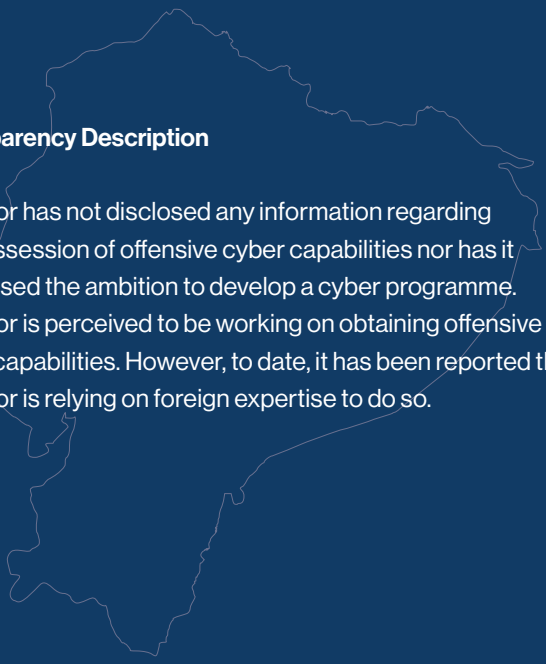
Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■☐☐☐

Organization for Offensive Cyber (2020):	Comando de Ciberdefensa
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	35.06 (89th)
Internet Penetration (2020)	65%
Internet Freedom Score	62/100 (Partly free)

Transparency Description

Ecuador has not disclosed any information regarding the possession of offensive cyber capabilities nor has it expressed the ambition to develop a cyber programme. Ecuador is perceived to be working on obtaining offensive cyber capabilities. However, to date, it has been reported that Ecuador is relying on foreign expertise to do so.



Declared Capability Rating

Score ☐☐☐☐☐

No indications of a declared cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■☐☐☐

Perceived to be working on obtaining offensive cyber capabilities. Ecuador appears to rely on foreign expertise to this end. Overall, very little reports were found that described the nation's cyber power.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"Ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021," Jácome Guerrero Juan Carlos, September 2020.	The document notes the lack of a national cyber defence strategy and the inability of the current cyber-defensive structure to prevent cyberattacks against national critical infrastructure. This is due in part to the reduced budget allocated to cyberdefence. [Original: la infraestructura de ciberdefensa con la que actualmente cuenta nuestro país y las FF.AA., es insuficiente para el cumplimiento de sus misiones. Quedando en evidencia la vulnerabilidad de la infraestructura crítica nacional, a los ataques cibernéticos. Siendo entre otras causas, una consecuencia de un presupuesto reducido para ciberdefensa.] The article also mentions that there are not enough cybersecurity experts in the armed forces to counteract a potential attack [Original: Las Fuerzas Armadas, en la actualidad, no cuentan con suficiente personal capacitado en Ciberdefensa y el existente no tiene una articulación intra - fuerzas.] Level 0
"Armed Forces will have a Cyber Defense Command", Ecuador Times, September 2014	Reports that the Armed Forces will have its own Cyber Defence Operations Command from 2015, which will cost about eight million dollars. Level 0
"As cyberwarfare heats up, allies turn to U.S. companies for expertise," Ellen Nakashima, November 22 2012.	Alleges that Ecuador has turned to Cuba to help them develop offensive cyber capabilities (where they were trained by top Russian officials). Level 2

Egypt

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■☐☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020):	Ranked as 30th (last) both overall and when it comes to offense
National Cybersecurity Index (2022)	57.14 (50th)
Internet Penetration (2020)	72 %
Internet Freedom Score	26/100 (Not free)

Transparency Description

Egypt's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. Egypt has not official disclosed to be in possession of offensive cyber capabilities. Very little public information about Egyptian offensive cyber programme is currently available and Egypt is perceived as to be mostly focusing on acquiring spyware tools from foreign vendors for domestic surveillance and espionage operations.

Declared Capability Rating

Score ☐☐☐☐☐

No indications of a declared cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Document	Excerpt
"National Cybersecurity Strategy 2017-2021," Ministry of Communications and Technology, 2017.	Does not mention offensive capabilities, or aspirations thereof. Only focused on national defence. Level 0

Perceived Capability Rating

Score ■☐☐☐☐

Egyptian capabilities are perceived to be mostly limited to authorities acquiring spyware from foreign vendors for domestic surveillance and espionage operations.

Data availability rating (1 being highest number of sources, 21 lowest): **17/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Ranked Egypt as #30 of the 30 countries included. This also included a last-place finish in the metric of offense. However, the report did note that "It was also very difficult to find information on the role and priorities of the Egyptian military and intelligence community," (P. 33). Level 0

Document	Excerpt
"Egypt Is Using Apps to Track and Target Its Citizens, Report Says," Ronen Bergman and Declan Walsh, October 4 2019.	This cyber operation was conducted against their own citizens, where the Egyptian Ministry of Communications and Information Technology and the General Intelligence Service had installed apps on phones which tracked location and conversations. **Level 1**
"IDF: Egyptian cyber warfare in Sinai causing cell disruptions in south Israel," Anna Ahronheim, March 2 2018.	This article details how the Israeli Defence Forces claimed that the Egyptian army has been causing cellular blackouts in southern Israel. This was not supposed to target Israel: apparently Egypt was using this technology against Islamic State terrorists. **Level 1**
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	Egypt has acquired surveillance and intelligence tools on several occasions from Italian company Hacking Team. **Level 1**
"Egypt, FinFisher Intrusion Tools and Ethics," F-Secure Labs, March 8 2011.	During the Arab Spring, protesters in Egypt took over the offices of the Egyptian State Security in which they found contracts for the sale of FinFisher, potentially linking the state to the purchase of spyware. **Level 1**

Estonia

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber (2018)	Cyber Command
National Cyber Power Index (2020)	Ranked 14th overall and 11th when it comes to offense
National Cybersecurity Index (2022)	90.91 (5th)
Internet Penetration (2020)	89%
Internet Freedom Score	94/100 (Free)

Transparency Description

Estonia's scores for the declared and perceived capability rating only differ slightly at the middle-end of the spectrum. While Estonian security concept (2017) and strategy (2019) recognise cyber warfare as part of the military defence and adopt a whole-of-nation approach to cybersecurity by involving actors from the private sector, official documents don't specifically mention offensive measures and it seems that the use of cyber capabilities is part of a broader deterrence posture. However, in 2018 Estonia established a Cyber Command and its website appears to hint at an offensive capability. Indeed, it contains relevant information and a high-level overview of the command's structure and tasks, as well as to various subunits, such as the Command Centre, the Planning Team, CERT capabilities, a Cyber Operations Group, and a Cyber Range. Estonia is broadly considered a digital leader. Its cyber arsenal is perceived to include offensive capabilities, which sources link to the "cyber operations" branch of the Cyber Command with the task to carry out delf-defence countermeasures. While there is no public record of past cyber operations by Estonia, its military forces publicly detail their participation in NATO exercises.

Declared Capability Rating

Score

Estonian offensive cyber capabilities are phrased as being part of its countermeasures in case of self-defence rather than overtly offensive weapons. To this end, it also takes on a whole of nation approach that enables government and non-state resources.

Data availability rating (1 being highest number of sources, 10 lowest): **7/10**

Document	Excerpt
Website Estonian Cyber Command, last accessed January 2022	The website of the Estonian Cyber Command, established in August 2018, offers a high-level overview of the command structure and tasks, which includes a "Cyber and Information Operations Centre" that is responsible for planning and organising such operations. It includes subunits, such as a Command Centre, Planning Team, CERT capability, Cyber Operations Group, and a Cyber Range – implying an offensive capability. **Level 3.5**
"Summary of Estonia's Position On How International Law Applies in Cyberspace – Ministry of Foreign Affairs," Estonia, 2020.	Estonia believes that "States have the right to respond to malicious cyber operations, including using diplomatic measures, countermeasures, and, if necessary, their inherent right of self-defence." **Level 0**

Document	Excerpt
"Cybersecurity Strategy 2019-2022," Ministry of Economic Affairs and Communications, 2019.	The national cybersecurity strategy notes Estonia's need for international cooperation on cyber deterrence and collective countermeasures, albeit not specified if these efforts also extend to the use of offensive measures. **Level 0**
"National Security Concept 2017," Kaitseministeerium, 2017.	"Cyber warfare is an integral part of military defence and cyber security. The private sector and volunteers will be involved in these activities." (P. 12) **Level 3**

Perceived Capability Rating

Score ■■□□□

Estonia is perceived as a digital leader, which comes with an expectation that, in theory, it is expected to have an offensive cyber capability. However, very little public information was found that describes this capability and is mostly limited to coverage about the Cyber Defence League, Cyber Command, and its participation in international exercises. No public reports were found that describe past Estonian cyber operations.

Data availability rating (1 being highest number of sources, 21 lowest): **20/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	The index ranked Estonia in 14th place overall and 11th with regard to offence. **Level n/a**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	Estonia is one of the NATO nations which has a Cyber Command, which organises the preparation of wartime and reserve forces, as well as conscript service in the area of cyber defense (P. 192). It is expected to have 300 cyber combatants by 2023 (P. 194). **Level 2**
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	The Author notes that Estonia has not been interested in conducting offensive cyber operations until October 2018, when it established a military cyber command. (p. 10) **Level 2**

Ethiopia

Cyber Transparency Score	**Transparent and Low Capability**
Declared Capability Rating	■□□□□
Perceived Capability Rating	■□□□□

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	32.47 (95th)
Internet Penetration (2020)	24%
Internet Freedom Score	27/100 (Not free)

Transparency Description

Ethiopia's scores for the declared and perceived capability are identical at the lower-end of the spectrum. To date, Ethiopia's plans to develop offensive cyber capability, as well as to integrate them within its military command, appear to be aspirational. From the outside, Ethiopia's cyber capabilities are perceived to be limited to spyware tools acquired from foreign vendors and used to monitor news and dissident sites, to suppress independent reporting, and to impose the regime's monolithic views.

Declared Capability Rating

Score ■□□□□

Stated aspiration for offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **9/10**

Document	Excerpt
"Cyber warfare: Threat of the time Ethiopia's plan to set up Cyber Security Force timely, pre-empt action," Ethiopian Press Agency, December 14, 2018.	"Ethiopia revealed its plan to establish cyber military force to prevent cyberattacks, an imminent threat which even most developed countries have also been experiencing with rise of sophisticated hackers and attackers." Level 1
"Ethiopian PM says military reform to embrace cyber security, space force," Xinhua, November 8, 2018.	"With regard to the legal framework, the revisions made look at including the structure of the Navy within the Defence Force Proclamation, and will in the future include Cyber Security and Space Force considerations," the statement reads. According to Ahmed, the reform is being made with due emphasis given to the context of building modern warfare units, which include land, air, seas, cyber and space." A Defence Force that can readily meet this context is in the process of being built," the statement quoted Ahmed as saying." Level 1

Perceived Capability Rating

Score ■□□□□

Ethiopia's offensive tools are limited to spyware acquired from foreign vendors used to surveil domestic and foreign dissidents.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware," Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert, December 6 2017.	CitizenLab shows that Ethiopia also acquired spyware tools from Israeli surveillance firm "Cyberbit", also to target Ethiopian dissidents abroad. Level 1
"Hacking Team Breach Shows a Global Spying Firm Run Amok," Andy Greenberg, July 6 2015.	Notes that Ethiopia has purchased spyware tools from Italian surveillance firm "Hacking Team". Level 1
"Enemies of the Internet 2014 - Ethiopia: Full online powers," Reporters Without Borders, March 12 2014.	This report alleges that the Ethiopian cybersecurity network, INSA, "uses aggressive spyware to monitor news sites and dissident sites, suppress independent reporting and impose the regime's monolithic views." These powers are also allegedly used against citizens living abroad. Level 1

Finland

Cyber Transparency Score Transparent and Low Capability

Declared Capability Rating ■■□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber (2018)	
Cyber Division of the Finnish Defence Forces C5 Agency	
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	85.71 (10th)
Internet Penetration (2020)	92%
Internet Freedom Score	n/a

Transparency Description

Finland's scores for the declared and perceived capability rating are identical at the lower-end of the spectrum. Finland has not officially declared to be in possession of offensive cyber capabilities. However, its strategies explicitly underscore the importance of adopting 'proactive measures' in cyber defence, as well as the aspiration to develop a comprehensive cyber arsenal which includes a 'cyber-attack capability'. In this regard, in the occasion of the establishment of a cyber subdivision of the Finnish Defence Forces C5 Agency in 2018, the Commander of the Finnish Defence Forces stressed that cyber defence will inevitably involve the ability to attack. Beyond that, no official information regarding core operational principles or military doctrine has ever been disclosed. From the outside, Finland's capabilities are perceived as mostly aspirational, in line with what the government has disclosed so far, and no offensive operations have ever been attributed to Finland.

Declared Capability Rating

Score ■■□□□

Finland has disclosed that it has ambitions to develop concrete offensive cyber capabilities, but no further details have been disclosed since the nation established a Cyber Unit in 2015. In contrast to some of its European counterparts, Finland does not have a strict "Cyber Command", but instead has a Cyber Defence Division within he Finnish Defence Forces C5 Agency. Furthermore, the traditional military branches (army, air force and navy) have integrated cyber defence capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"Implementation Programme for Finland's Cyber Security Strategy for 2017–2020," The Security Committee.	"In accordance with the Cyber Security Strategy the Defence Forces will develop and maintain a comprehensive cyber defence capability for their statutory tasks. This also includes a cyber-attack capability." Level 2
The Finnish Defence Forces will establish a new cyber unit – prepare for hybrid wars by strengthening cyber defences, YLE, 25 September 2014	In an interview, the Commander of the Finnish Defence Forces, General Jarmo Lindberg, explains that a cyber unit will be established, explaining that "In the future, cyber defence will inevitably also include the ability to attack, as its own systems will be tested specifically through training attacks." Level 1
"Finland's Cyber Security Strategy," Secretariat of the Security Committee, 2013.	"The Defence Forces will protect their systems in such a manner that they are able to carry out their statutory tasks irrespective of the threats in the cyber world. Guaranteeing capabilities, intelligence and proactive measures in the cyber world will be developed as elements of other military force." Level 2

Perceived Capability Rating

Score 

Finland's perceived capabilities are limited to secondary sources observing the government's stated aspiration to develop offensive capabilities. Finland has also not been attributed to any offensive actions.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	Observes that "Finland has a cyber defence division, but no cyber command. ... It has developed a classified a concept of cyber defence but (yet) without elevating its cyber operational arm, authorized to develop also offensive capabilities, to a command." (P. 188). **Level 2**
"Preparing for Cyber Conflict Case Studies of Cyber Command," Piret Pernik, December 2018.	This document implies that Finland does have offensive cyber capabilities through outlining the command structure of cyber power in Finland. Basically, the decision for Finland to participate internationally in crisis management is made by the President, who is advised by his security council. "This regulation also pertains to the deployment of offensive cyberspace capabilities as part of international deployments." (P. 9). Claims the Finnish cyber division has 100-200 people and is working on refining its ability to conduct offensive cyber operations, but doesn't include information operations or electronic warfare (P. 24). **Level 2**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	This 2011 report details some plans that Finland had for their offensive cyber capabilities. Notably, they write that a government plan "increases funding for the military's Cyber Defence Unit to allow it to mount cyber-attacks on "hostile forces" as part of a "Credible Response Platform", which is likely to deploy malware, worms, and viruses against "attackers". The initial stages of the plan could be operational by 2013." (P. 20-21). **Level 2**

France

Cyber Transparency Score Transparent and High Capability

Declared Capability Rating ■■■■□

Perceived Capability Rating ■■■■□

Organization for Offensive Cyber (2017)	Commandement de la cyberdéfense (COMCYBER)
National Cyber Power Index (2020)	Ranked 6th with a score of 23.43 and 10th when it comes to offense)
National Cybersecurity Index (2022)	84.42 (11th)
Internet Penetration (2019)	85%
Internet Freedom Score	78/100 (Free)

Transparency Description

France's scores for the declared and perceived capability rating are identical at the higher-end of the spectrum. France has disclosed to be in possession of offensive cyber capabilities. While prior to 2017 official information was mostly focused on 'active defence' capabilities, in 2017 France established a Cyber Defence Command (COMCYBER), whose tasks are to protect the information systems of the armies, as well as to design, plan and conduct military operations in cyberspace. In 2019, France also published its Military Cyber Doctrine, which consists of the *Ministerial Policy for Defensive Cyber Warfare* and the *Public Elements for the Military Cyber Warfare Doctrine*. The doctrine expressly integrates cyber activity within conventional military operations, and the General Directorate of Armaments (DGA) - which cooperates with the CYBERCOM - is entrusted with developing offensive computer warfare capabilities. France is widely perceived as a cyber power. A 2021 public report argues that, despite there being little public evidence of destructive cyber operations by France, its robust retaliatory responses in the context of national cyber security demonstrate a high-level capability. With regard to past offensive operations, an APT known as Animal Farm has been attributed to France.

Declared Capability Rating

Score ■■■■□

France's most significant public disclosure on offensive cyber capabilities occurred through its military cyber strategy in January 2019. The strategy consists of two separate documents: the *Ministerial Policy for Defensive Cyber Warfare* and the *Public Elements for the Military Cyber Warfare Doctrine*. Together, these documents outline the French Ministry of Defence's doctrine on defensive and offensive cyber operations. Prior to that, official government information was mostly oriented around 'active defence'. Another strategic shift is the separation of offensive cyber capabilities from the intelligence silo, which are now coordinated by the French Cyber Defence Command (COMCYBER), established in 2017.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"Le COMCYBER," Ministeres des Armees, January 26 2022.	The Cyber Committee (COMCYBER) is formed by more than 3.400 cyber-combatants who carry out both defensive and offensive cyber military operations. **Level 3**
"Éléments publics de doctrine militaire de lutte informatique offensive," Ministeres des Armees, 2019	"From now on, the Ministry of the Armed Forces has capacities and a doctrine of employment that covers cyber-offensive actions dedicated to the engagement of the armed forces." (P. 4) "the development of offensive computer warfare capabilities for the benefit of the armed forces is entrusted to the General Directorate of Armaments (DGA), as with any other military capability. Due to the sensitivities and dynamics of this field, COMCYBER teams and DGA cyber teams are working closely together to develop and implement a capability Road Map." (P. 11) [Original: Désormais, le ministère des Armées dispose de capacités et d'une doctrine d'emploi qui couvrent les actions offensive cybers dédiées à l'engagement des forces armées. [...] Le développement des capacités de lutte informatique offensive au profit des armées est confié à la direction générale de l'armement (DGA), comme pour toute autre capacité militaire. En raison de la sensibilité et de la dynamique du domaine, les équipes du COMCYBER et les équipes cyber de la DGA travaillent en étroite coopération à l'élaboration et à la mise en œuvre d'une feuille de route capacitaire.] **Level 4**
"France's New Offensive Cyber Doctrine," Arthur P.B. Laudrain, February 26 2019.	In recent years, France has become much more open about its offensive cyber operations policy. The 2019 offensive doctrine, which integrates cyber activity into conventional military operations is the latest development. Referencing Russian threats, ministers said that "France is "not afraid" of using cyber weapons... France did not wait until now to perform or even publicly admit doing so." "But so far, offensive cyber operations for purposes other than self-defence have been absent from public sight." Other publications also note this shift: "By publicly outlining its [offensive] doctrine, France assumes the posture of a cyber power, sending a message to allies and partners, as well as to potential attackers." That document also states that "France ... will cooperate on some aspects of offensive cyber warfare but will always maintain full control over its operations and capabilities, which "remain within the scope of its strict sovereignty."" **Level 3**
"Revue stratégique de cyberdéfense," SGDSN, February 2018.	The strategic review acknowledges that France has developed increasingly "active and aggressive" (P.34) cyber capabilities and that it intends to pursue active defence. One of the six missions is described to be a 'reaction' to cyber threats, including counterattack and repression of cyber threats. **Level 3**
"Livre Blanc Défense et Sécurité Nationale," Direction de l'information légale et administrative, Paris, 2013	The document talks about the necessity of being ready to offensively respond to a cyberattack and France's willingness to develop sophisticated offensive cyber capabilities. **Level 1**

Perceived Capability Rating

Score 

France is perceived as a cyber power based on references to self-disclosures by the French government about their willingness to use offensive capabilities and their integration in the French military structure. In practice, most information about past operations is limited to the APT group Animal Farm, which was attributed to the French government, that carried out multiple surveillance operations against other nations, including Iran and Canada.

Data availability rating (1 being highest number of sources, 21 lowest): **10/21**

Document	Excerpt
"Cyber Capabilities and National Power" IISS, June 28 2021.	The IISS believes that "Although there is little public evidence of France carrying out other destructive cyber operations, its record of robust retaliatory responses in national-security situations suggests it is prepared to do so in certain circumstances, as its leaders have acknowledged." (P.63) Thus the report concludes saying that "France (...) [is believed to have]a considerable offensive cyber capability" (P.63) Level 4
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	France is ranked 6th overall and number 10 on the offensive metric. Level n/a
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The book predicts that France is to grow its cyber combatant force to 4000 by 2025 (P. 194). Moreover, France is also planning to spend 2.1 billion euros in establishing their cyber command. For comparison, the Netherlands spent 50 million euros in establishing theirs, with a yearly budget of 20 million (P. 194). Level 4
"NATO cyber-operations center will be leaning on its members for offensive hacks," Cyberscoop, August 2019.	France has signed on to offer their capabilities for the new NATO cyber operations center. This is commonly known as the Sovereign Cyber Effect Provided Voluntarily by Allies (SCEPVA). Level 4
"France's New Offensive Cyber Doctrine," Arthur P.B. Laudrain, February 26 2019.	In recent years, France has become much more open about its offensive cyber operations, particularly through its new doctrine, which integrates cyber activity into conventional military operations. Referencing Russian threats, the French Defence Minister Parly said that "France is "not afraid" of using cyber weapons. France did not wait until now to perform or even publicly admit doing so. "But so far, offensive cyber operations for purposes other than self-defense have been absent from public sight." Level 3
"Shouting at Americans: A Peek Into French Signals Intelligence," Alex Grigsby, September 15 2016.	The article details the Operation Babar or Operation Snowglobe as it is known by Canada. This was attributed to the Animal Farm APT, confirmed to be the French government, that targets governments, companies, media organisations, military contractors, and humanitarian organisations." First reported in 2014, and mainly operated for espionage. It is suspected to have targeted the following states: Syria, United States, Netherlands, Russia, Spain, Iran, China, Germany, Algeria, Norway, Malaysia, Turkey, United Kingdom, Ivory Coast, and Greece. In 2014, the former head of the French intelligence agency, made a polemic speech where he confirmed that the French government was behind the Animal Farm malware which targeted Iran's nuclear programme in 2009 (and also some computers in Canada). Level 1

Document	Excerpt
"Animal Farm APT and the Shadow of French Intelligence," Pierluigi Paganini, July 8 2015.	In 2015, researchers found a strain of malware labeled Babar which was traced back to the General Directorate for External Security (DGSE), France's external intelligence agency. The malware is also called Snowglobe by the Canadian Intelligence service. This malware is a potent espionage tool, able to monitor user's conversations and activity on the web. The link to the French government first came to light in "one of the documents leaked by the NSA whistleblower Edward Snowden, the slides were made by the Canadian intelligence agency and linked Babar to the French Government." The documents incriminated the government with having launched an espionage campaign in 2009 against the Atomic Energy Organisation of Iran, the Iran University of Science and Technology and two Tehran schools heavily involved in nuclear research, Malek-E-Ashtar University of Technology and Imam Hussein University. To a lesser extent, Babar also targeted Canada, Spain, Greece, Norway, Ivory Coast, and Algeria. In 2015, a spyware named Casper was found to be compromising a Syrian government website. This attack was attributed to a French state-sponsored APT for its sophistication and similarity to the Babar malware. **Level 3**
"Dino – the latest spying malware from an allegedly French espionage group analyzed," ESET, June 30 2015. (1) "Animal Farm APT and the Shadow of French Intelligence," Pierluigi Paganini, July 8 2015. (2)	In 2014, another malware was discovered when the French media released new slides from the Snowden leak. The new malware dubbed Dino was discovered to have targeted Iran. Dino could search for specific files, upload files to the command and control (C&C) server, and download further files from the control architecture (...) [it could] also schedule commands to be executed at a specified time, ... kill processes and uninstall the malicious code from the infected system to avoid leav[ing] traces of its presence" (2). The malware was developed by native French speakers and the Canadian intelligence services attributed with moderate certainty this attack to the French intelligence services. **Level 4**
"The Role of Offensive Cyber Operations in NATO's Collective Defence," James A. Lewis, 2015.	Mentions France alongside the US and the UK as the only NATO powers that currently (i.e. 2015) have the ability to undertake offensive cyber operations. **Level 3**
Cyphort Labs, December 16 2014.	Another malware tool bearing similarities to Babar and Casper was discovered in 2014 labeled EvilBunny. "The EvilBunny malware was originally delivered through a malicious PDF document" exploiting a vulnerability. "After successful exploitation the malware dropper would be loaded onto the system and infect the machine with EvilBunny." This malware was able to "evade detection" by "detect[ing] installed anti-virus- and firewall solutions." **Level 4**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	Outlines how, as of 2011, "France is also developing an offensive cyberwar capability under the purview of the Joint Staff and specialized services. Both the army and the air force have electronic warfare units. Offensive capabilities are also being pursued by the intelligence services." (P. 22). **Level 2**

Germany

Cyber Transparency Score	**Higher Declared Capability**
Declared Capability Rating	■■■□□
Perceived Capability Rating	■■□□□

Organization for Offensive Cyber (2017)	Cyber and Information Space Command
National Cyber Power Index (2020)	Ranked 7th overall and 4th when it comes to offense
National Cybersecurity Index (2022)	90.91 (6th)
Internet Penetration (2020)	90%
Internet Freedom Score	79/100 (Free)

Transparency Description

Germany's scores for the declared and perceived capability rating only differ slightly in the middle of the spectrum. While having declared to be in possession of offensive cyber capabilities, the 2021 Cyber Strategy, echoing the previous one from 2015, states that offensive capabilities constitute an integral part of cyber defence. Furthermore, in 2017, Germany established a Cyber and Information Space Command, which is responsible for the preparation, planning, and implementation of offensive and defensive cyber military operations. In light of the strict constitutional restraints upon military operations, Germany has not published any military cyber strategy or doctrine, therefore lacking details about its missions, conditions and principles of employment, as well as how such capabilities integrate within the overall military command. Accordingly, due to the limited details disclosed and to the limited mandate of German Armed Forces, Germany's offensive cyber capabilities are perceived as relatively limited. No offensive operation has ever been overtly attributed to Germany.

Declared Capability Rating

Score ■■■□□

Germany's cybersecurity strategy from 2016, updated in 2021, refers to the existence of offensive cyber capabilities. Its Cyber Operations Center (ZCO) established in 2017, is responsible for the preparation, planning, and implementation of offensive and defensive cyber military operations. However, the German constitution limits military cyber operations due to its stringent legal restrictions. The absence of comprehensive disclosure of German capabilities since 2016 is not perceived to be a matter of secrecy, but as an absence of an overarching strategic doctrine.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"Cybersicherheitsstrategie für Deutschland 2021", Bundesministerium des Innern, 2021	"Cyber-Defence in the Bundeswehr comprises defensive and offensive abilities for working in cyberspace, within its constitutional mandate, which are suitable for the conduct of operations." (P. 133) [Original: Cyberverteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und der vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyberraum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind (...)] **Level 3**

Document	Excerpt
"Cyber-Sicherheitsstrategie für Deutschland," Bundesministerium des Innern, 2016.	"Cyber-Defense includes the defensive and offensive abilities to work in cyberspace in the Bundeswehr within the framework of its constitutional mandate and international legal framework." (P. 46) [Original: Cyber-Verteidigung umfasst die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und dem völkerrechtlichen Rahmen vor- handenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum] **Level 3**
"Drucksache 18/6989 Antwort der Bundesregierung" Deutscher Bundestag, December 10 2015.	"The use of military cyber capabilities by the Bundeswehr is subject to the same legal requirements as any other deployment of German armed forces." (P. 4) The document goes on to mention the use of cyber capabilities during deployments abroad (P.3). [Original: "Der Einsatz militärischer Cyber-Fähigkeiten durch die Bundeswehr unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte"]. **Level 3**

Perceived Capability Rating

Score ■■□□□

Germany's offensive cyber capability is perceived to be relatively low, with limited details on its military cyber command centre and no public record of past German cyber operations, with the exception of commercial spyware that the German police acquired in 2013.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Germany is ranked 4th on the offense capability metric and ranked 7th overall. **Level n/a**
"German Military Cyber Operations are in a Legal Gray Zone," Matthias Schulze, April 8 2020.	The author calls German approaches 'limited offensive cyber operations'. **Level 2**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	Considers the German cyber command to be well-developed, being in the 'growth' stage and having a workforce of 13000 (P. 192). This should expand to 14500 by 2021 (P. 194). **Level 2**
"Germany Develops Offensive Cyber Capabilities Without A Coherent Strategy of What to Do With Them," Matthias Schulze and Sven Herpig, December 3 2018.	Schulze and Herpig (2018) observe that Germany has been slowly moving towards offensive cyber activity. One thing they point at is the creation of a cyber innovation agency, which is similar to the US's DARPA. This could potentially create cyber projects (and tools for cyber offence). This suggests that Germany is perceived to have capable offensive cyber power tools, but lacks a coherent strategy that guides their use. **Level 2**
"Secret Government Document Reveals: German Federal Police Plans To Use Gamma FinFisher Spyware," Andre Meister, January 16 2013.	In one instance, the German federal police was found to have acquired surveillance and intelligence tools from private vendor FinFisher Gmbh. **Level 1**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	"The Department of Information and Computer Network Operations of the armed forces' Strategic Reconnaissance Unit is tasked with developing cyber capabilities. In 2009, this consisted of 76 military personnel with computer science training provided by the armed forces. The unit was reportedly designed as a specialized cyber group to be trained in offensive cyber capabilities," (P. 24-25). **Level 2**

India

Cyber Transparency Score Untransparent

Declared Capability Rating ■□□□□

Perceived Capability Rating ■■■□□

Organization for Offensive Cyber (2018)	Defence Cyber Agency
National Cyber Power Index (2020)	Ranked 21st overall and 28th when it comes to offense
National Cybersecurity Index (2022)	59.74 (46th)
Internet Penetration (2020)	43%
Internet Freedom Score	49/100 (Partly free)

Transparency Description

A lack of transparency is observed for India. While the latest military doctrine (2017) identifies cyberspace as a domain of warfare in line with the previous doctrine from 2004, which mentioned offensive cyber capabilities as part of "Information Warfare" and included electronic warfare, no details have ever been disclosed yet. It is still unclear to what extent Indian cyber capabilities are aspirational or established. However, India is perceived as possessing offensive cyber capabilities, as well as to be increasingly investing resources in developing them. A new military cyber doctrine is reportedly under development since 2019. At the same time, several cyber operations have been attributed to India, and a significant number of APTs are suspected to be affiliated with the Indian government.

Declared Capability Rating

Score ■□□□□

Stated aspiration for offensive cyber capabilities. India has established a Defence Cyber Agency in September 2018, which was reportedly operational by August 2021. While the 2004 Army Doctrine mentions offensive cyber capabilities as part of 'Information Warfare' and includes electronic warfare, it remains unclear to what extent these capabilities remain aspirational or established. A military cyber doctrine was under development from 2019 onwards, but it's unclear if it has come to fruition.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"India's New Defence Cyber Agency Will Have to Work Around Stovepipes Built by Army, Navy & Air Force: Lt Gen DS Hooda", News18, June 26 2019	In an interview the head of the new Cyber Defence Cyber Agency, Lt Gen DS Hooda, explained that a doctrine for cyber-warfare will be drawn up. Level 0
"Indian Army Land Warfare Doctrine," Indian Army, 2018.	The doctrine stresses the intention of developing cyber-deterrence capabilities: "The Indian Army will upgrade existing Cyber Warfare capabilities with the objective to develop cyber deterrence and defence capabilities, while simultaneously devising means of eliminating such threats." (P.10) Level 1
"Joint Doctrine Indian Armed Forces" Indian Armed Forces, April 2017.	In the doctrine cyberspace is identified as a domain of warfare, but there is no mention of developing offensive cyber capabilities. Level 0

Document	Excerpt
"National Cyber Security Policy," Government of India, July 2 2013.	"Prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions." (P.4) Level 0
"Indian Army Doctrine (part one)," UNIDIR, October 2004	"Cyber Warfare: This entails techniques to destroy, degrade, exploit or compromise the enemy's computer-based systems. Cyber warfare includes exclusive attacks, known as hacking, on enemy computer networks. Computer hacking has evolved to a stage wherein information stored or passing through computer networks is interfered with to degrade the adversary's C2 structure. Influence perceptions, plans, actions and the will of adversaries to oppose own and friendly forces by offensive employment of information warfare techniques." (P. 21) Level 1

Perceived Capability Rating

Score ■■■□□

India is increasing investments in cyber capabilities – both defensive and apparently offensive. However, many observers remain skeptical about how committed or impressive Indian capabilities are. While several cyber operations have been attributed to India, it remains unclear to what extent the military has integrated this capability within its overall military structure and used it to achieve strategic objectives.

Data availability rating (1 being highest number of sources, 21 lowest): **5/21**

Document	Excerpt
"India, new destroyer of regional cyber stability – China Military," Lu Chuanying, November 25 2021.	The article reports on an attack waged against China and other countries in the South Asian subcontinent. The article notes that a Chinese cybersecurity report attributes the attacks to a group in India: "it can be seen from the report that the organization is obviously backed by state forces of India." Level 3
"Analysis of the young elephants' cyberattack activities in South Asia," Antey Cert, November 19 2021.	The APT, denoted "baby elephant" by the firm, is a cyberespionage group suspected to originate in India. The company has been recording attacks by this group since 2017. According to the report, the attacks have grown in sophistication over the years to become "the most active and mature attack group in South Asia" [Original: 如今该组织已成长为南亚地区最为活跃和成熟的攻击组织]. Further explaining that "its exposure, the number of attacks and targets has continued to grow rapidly. Compared with the early unstructured exploration attempts, the organisation has now formed several sets of fixed tool combination models." [Original: 相比于早期未成章法的探索尝试，如今该组织已形成了几套较固定的工具组合模式，可供]. Although from 2017 to 2020 the scope of targets involved governmental and defence agencies in various South Asian countries (Nepal, Pakistan, Sri Lanka, etc.), by 2021, the attacks started targeting Chinese agencies: "targeted intelligence theft campaigns were conducted against relevant Chinese agencies" [Original: 向中国的相关机构进行情报窃取的定向攻击活动] Level 3
"Private Israeli spyware used to hack cellphones of journalists, activists worldwide," Dana Priest, Craig Timberg and Souad Mekhennet, July 18 2021	In one instance, India was found to have acquired surveillance and intelligence tools from Israeli private company NSO. Level 1

Document	Excerpt
"Cyber Capabilities and National Power," IISS, June 28 2021.	The IISS underlines how India has been developing offensive cyber capabilities to be used against Pakistan. However, it also acknowledges the need for India to further develop its capabilities in order to be able to deliver effective and sophisticated cyberattacks. **Level 3**
"India: An Emerging Cyber Powerhouse With a Booming Cybercriminal Underground," Insights, October 2020	"It was not until 2019 that the Defense Cyber Agency (DCA), a new tri-service agency for cyber warfare, was established. It is said to have more than 1,000 experts who will be distributed into a number of formations in the Army, Navy, and Indian Air Force (IAF). The DCA's goal is to become capable of hacking into networks, mounting surveillance operations, and laying honeytraps. The agency seeks to build a state-of-the-art lab that can recover deleted data from hard disks and cellphones, break into encrypted communication channels, and perform other complex objectives. As the tension between India and China grows, it is clear that cyber warfare and espionage will be at the forefront of any conflict that arises." (P. 7) **Level 2**
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	India is ranked 21st most comprehensive cyber power and 28th (out of 30) for offensive cyber abilities.
"Pakistan's Intelligence Agencies have identified a major cyber-attack by Indian Intelligence Agencies involving a range of cybercrimes including deceitful fabrication by hacking personal mobiles and technical gadgets of government officials and military personnel," ISPR, August 12 2020.	Pakistani attribution of 2020 cyberattack to India: "Pakistani intelligence agencies have tracked a major security breach by Indian hackers whereby phones and other gadgets of government officials and military personnel were targeted. (...) According to a statement by the Inter-Services Public Relations (ISPR), the cyberattack by Indian intelligence agencies involved "a range of cybercrimes including deceitful fabrication by hacking personal mobiles and technical gadgets"." **Level 3**
APT-04/APT-C-17 (aka Rattlesnake, T-, SideWinder, Hardcore Nationalist (HN2)). According to reports, this APT could potentially be either cybercriminal or affiliated with the Indian State "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "First Binder Exploit Linked to SideWinder APT Group," Ecular Xu and Joseph C Chen, January 6 2020. (2)	The group could potentially be affiliated with India. The group usually attacks Pakistani military targets. One campaign by the group was discovered in 2019. The campaign used malicious Google Play Store apps to gather information on the victim's phone. **Level n/a**
"India's Response to China's Cyber Attacks," Elizabeth Radziszewski, Brendan Hanson, and Salman Khalid, July 3 2019.	The authors note how India has not been making sizeable investments in their cyber power capabilities – defence or offence. They quote a cyber security expert who, in 2017, stated that "The country [India], according to Tyagi, needs more time and money to improve defensive cyber capability and can't even contemplate using cyber as an offensive weapon." The only major changes they have noted so far is the establishment of the Indian Defence Cyber Agency, which has opened in November 2019. This is corroborated by other news reports. However, the authors also note: "But such an initiative may be insufficient to deter China given the meager spending devoted to cyber defence. Moreover, it is not entirely clear how relying on existing capabilities from the armed forces can limit attacks that have been undeterred by such capabilities." **Level 2**

Document	Excerpt
"The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5," Ryan C. Maness, June 1 2019.	The document lists one or two potential cyberattacks done by India in retaliation to Pakistan. However, I could not confirm these via unbiased (i.e. non-Pakistani) news or government sources.
"Agencies take shape for special operations, space, cyber war," The Times of India, May 16 2019.	This article describes that Rear Admiral Mohit Gupta will head the new Cyber Defence Cyber Agency, which is expected to become fully operational by October-November of 2019. **Level 0**
APT-C-09/ APT-C-35 (aka Patchwork, Dropping Elephant, Chinastrats, Monsoon, Quilted Tiger, Sarit, SectorE02, ZINC EMERSON, EHDevel, Manul, Confucius, Operation Hangover, TG-4410) "Patchwork APT Group Targets US Think Tanks," Matthew Meltzer, Sean Koessel, Steven Adair, June 7 2018. (1) "Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent," Brandon Levene, Josh Grunzweig and Brittany Barbehenn, March 7 2018. (2)	Patchwork is thought to be affiliated with the Indian State. The group seems to choose its targets in line with the strategic interests of India. Since 2015, it has targeted around 2,500 networks. Its victims are usually government officials working on military or political issues relating South East Asia and the South China Sea. For instance, in 2015, the group attacked an employee working on Chinese policy in a European organisation. Throughout 2016, it targeted victims in the within the Indian subcontinent. In 2018, another attack was recorded against a US think tank. **Level 3**
"New players join race for offensive cyber abilities," Oxford Analytica, August 20 2018. (1) "Patchwork," Mitre Attack, May 31 2017. (2)	The article alleges several cyber operations, including "Operation Hangover," which targeted a Norwegian telecommunications company and Chinese and Pakistani actors primarily for espionage purposes. They also mention another Indian cyber actor called 'Dropping Elephant.' Others claim that these attacks are in actuality associated to other prominent APT groups in the region (2). Regardless, these capabilities here all appear to be espionage- focused. **Level 1**
"Cyber Warfare and Pakistan," Jibran Ali, 2017.	The document speaks about India's increasing partnership with Israel to gain access to new and better cyberwarfare capabilities. **Level 2**
"The best among limited options," M.K. Narayanan, (Former NSA of India), September 21 2016.	"Perhaps, India's best option would be to engage in cyber sabotage and cyberwarfare, hiding behind the plausible deniability available in such attacks. Our capacity in this area is considerable, and it should be possible to engage in extensive cyber sabotage and cyberwarfare to bring Pakistan to its knees. This may be worth examining, instead of adopting 'tit for tat' methods with a 'rogue' nation." **Level 3**
"Unveiling Patchwork – The Copy-Paste APT," Cymmetria, 2016. (1) "Monsoon– Analysis of an APT Campaign," Andy Settle, Nicholas Griffin and Abel Toro, August 8 2016. (2)	Patchwork malware attacks are suspected to be affiliated to India. The attacks are mainly espionage-motivated, and targeted at military and the private sectors in India's neighbouring countries notably Bangladesh, Pakistan, and Sri Lanka. **Level 3**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	India's Ministry of Defence coordinates cybersecurity responses. They have a department, the Defence Information Warfare Agency, which coordinates information warfare (P. 28). **Level 2**

Indonesia

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■☐☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	38.96 (83rd)
Internet Penetration (2020)	54%
Internet Freedom Score	48/100 (Partly free)

Transparency Description

Indonesia's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. Indonesia has not officially declared to be in possession of offensive cyber capabilities. A 2021 article refers to the existence of an Indonesian Cyber Unit, the Satuan Siber (or Satsiber), established in 2017 within the Armed Forces. However, its mandate, offensive capabilities, structure, and core operational principles have not been disclosed yet. From the outside, very little public information is currently available with regard to Indonesia and its capabilities are perceived to be limited to domestic surveillance tools. However, it must be noted that sanctioned media in 2016 reported on a surveillance operation allegedly carried out by the Indonesian government against Australian servers.

Declared Capability Rating

Score ☐☐☐☐☐

No indications of a declared offensive cyber capability. Indonesia has a dedicated Cyber Unit within its Armed Forces, but its self-declared offensive capabilities remain undisclosed for now.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"TNI form Satsiber," KOMINFO, 2021.	This article refers to the Indonesian Cyber Unit, the Satuan Siber, or Satsiber that is established under the Armed Forces in October 2017: "TNI Commander General Gatot Nurmantyo said that various changes as a result of technological, information, and communication developments require the TNI to have cyber defense capabilities in order to increase deterrence and prevention of war or cyberattacks against the TNI and national cyber defense." Level 0
"Defence White Paper," Defence Ministry of Indonesia, 2015.	When referring to their defence capabilities, the document states: "Defence capabilities include air national defence, strategic strike, electronic warfare, and cyber defence." (P. 109). In turn, "The electronic warfare capability is prepared to support the military operations and training, which includes electronic warfare tools, human resources, and other supports. Cyber defence capability is developed to ensure cyber security for the benefit of the national defence capabilities, and integrated cyber with all the instruments of national power to reduce the risk of cyberattacks." (P. 110). Level 0
"Cyber defense Guidelines," Kementerian Pertahanan Republik Indonesia, 2014.	The guidelines acknowledge the need to develop counter-attack capabilities for the purpose of deterrence but expands no further on offensive capabilities. Level 0

Perceived Capability Rating

Score ■□□□□

Indonesia's cyber capabilities are limited to domestic surveillance, and while it has a dedicated Cyber Unit, the available public information suggests its offensive capability is weakly positioned compared to its regional counterparts.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"Cyber Capabilities and National Power," IISS, June 28 2021.	The report mentions Indonesian long-term plan to acquire offensive cyber capabilities but acknowledges that at the moment said capabilities are limited to domestic cyber surveillance limited in counter-terrorism operations. **Level 2**
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	This assessment of Indonesia's cyber capability refers to a White Paper in which it described cyber "as an asymmetric weapon for non-linear warfare and as an integrated support for military operations," (P. 41). It moreover mentions that Indonesia has been participating in cyberwar simulations with China. **Level 2**
"FinFisher spyware: Indonesian government 'using Sydney server for surveillance program'," Lisa Main and Conor Duffy, January 26 2016.	The article reports on a surveillance attack against Australian servers. The threat actor used FinFisher, an " intrusive spyware developed by Munich-based FinFisher Gamma Group" to infiltrate phones and computers and put them under surveillance. The article attributes the attack to the Indonesian government which is "one of the most avid users of FinFisher spyware." **Level 1**

Iran

Cyber Transparency Score Very Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■■■

Organization for Offensive Cyber: Islamic Revolutionary Guard Corp and the Cyber Defence Commando (Gharargah-e Defa-e Saiberi) (unconfirmed)

National Cyber Power Index (2020): Ranked 23rd overall and 8th in the metric of cyber offense

National Cybersecurity Index (2022)	14.29 (129th)
Internet Penetration (2020)	84%
Internet Freedom Score	16/100 (Not free)

Transparency Description

A lack of transparency is observed for Iran. The government has not officially declared to be in possession of offensive cyber capabilities nor has it declared aspirations. However, Iran is perceived as already possessing robust offensive cyber capabilities, and it is widely recognised as having launched several offensive cyber operations with disruptive and even destructive effects on targets. While still being less developed compared to top-tier cyber powers, Iran's cyber capabilities and overall experience in cyberspace are considered to display operational maturity. The Council on Foreign Relations has listed and detailed 44 cyber operations carried out or sponsored by Iran for various purposes since 2010, the year in which Iran was hit with the *Stuxnet* attack. While the bulk of its operations are not very sophisticated and mostly intended at espionage and data theft, some operations, like Shamoon or the one targeting Sands Casino, show more destructive traits. The Iranian offensive cyber programme is relatively new, but it is already integrated well within overall military structure and it purportedly offers some form of minimum deterrence *vis-à-vis* larger adversaries. However, no official information in this regard has ever been disclosed.

Declared Capability Rating

Score ☐☐☐☐☐

No indications of a declared offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■■■■

Iran is widely recognised to have acquired and used offensive cyber capabilities following the Stuxnet operation that targeted its nuclear enrichment programme. While the bulk of its operations are not especially sophisticated and mostly intended at espionage and data theft, some operations, like Shamoon or the one targeting Sands Casino, show more destructive traits. The Iranian offensive cyber programme is relatively new, but is already integrated well within overall military structure and national strategic goals. Iran even claims this offensive capability offers some form of minimum deterrence vis-à-vis larger adversaries. Past operations and state-sponsored APTs are well documented by many western governments and industry partners.

Data availability rating (1 being highest number of sources, 21 lowest): **3/21**

Document	Excerpt
"Cyber Capabilities and National Power," IISS, June 28 2021.	The IISS notes that "Overall, Iran has deployed offensive cyber for diverse goals and against a range of targets worldwide. Its cumulative experience now represents a relatively high level of operational maturity, with the regime's embrace of cyber operations firmly established as a useful instrument of national power." (P.120) Although there are different instances demonstrating the Iranian use of offensive cyber capabilities, it has to be noted that Iranian capabilities are significantly less developed in quality and scale than those of several states such as the US and UK and, regionally, Israel. **Level 4**
"Iran (Islamic Republic of)," UNIDIR Cyber Policy Portal, June 2021.	Iran has two cyber units, the Cyber Police of Islamic Republic of Iran (FETA) and the Cyber Defense Commando that potentially carry out offensive cyber operations. **Level n/a**
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Iran is ranked 8th in the metric of cyber offense and 23rd overall.
"Two Iranian Nationals Charged in Cyber Theft Campaign Targeting Computer Systems in United States, Europe, and the Middle East," US Department of Justice, September 16 2020.	In 2020, the US Department of Justice indicted two Iranian nationals for their role in a cyber intrusion campaign targeting computers in the US, Europe and the Middle East. At times, these operations were conducted on behalf of the IRGC. **Level 1**
"Cyber Operations Tracker," Council on Foreign Relations, 2020.	Lists and details 44 cyber operations sponsored by the Iranian state which date back to 2010. **Level 4**
"Iranian Offensive Cyber Attack Capabilities," Catherina A. Theohary, January 13 2020.	The author writes: "[Iran] has been developing technological cyber expertise as a form of asymmetric warfare against a superior conventional U.S. military." This move to develop their own offensive cyber weapons came after Iran was struck by the American-Israeli Stuxnet worm. "Following the discovery of the Stuxnet malware, U.S. assets experienced an increase in the severity and duration of cyberattacks originating in Iran." The document also identifies several Iranian bodies which are responsible for/ involved in offensive cyber operations: the Supreme Council of Cyberspace, the Islamic Revolutionary Guard Corps, the paramilitary Basij Cyber Council, and (in terms of countering) the National Passive Defense Organization. In addition, the paper discloses several proxies that Iran has been known to use. Finally, it identifies 4 forms of cyberattacks that Iran has been doing: website defacement, date breach/theft, denial of service, and destructive attacks. **Level 3**
"Explainer: How Iran's military outsources its cyber-warfare forces," Dorothy Denning, January 23 2020.	The article explains the structure of Iran's cyber power: "Iran's cyberwarfare capability lies primarily within Iran's Islamic Revolutionary Guard Corps, a branch of the country's military. However, rather than employing its own cyber force against foreign targets, the Islamic Revolutionary Guard Corps appears to mainly outsource these cyberattacks." It also notes that Iran uses both off-the-shelf malware and custom made tools. **Level 3**
"Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad," the Cybersecurity and Infrastructure Security Agency, June 30 2020. (1) "Troubled vision: Understanding recent Israeli–Iranian offensive cyber exchanges," JD Work and Richard Harknett, July 22 2020. (2)	Details some characteristics of Iranian cyber power: "Iranian cyber threat actors have continuously improved their offensive cyber capabilities. They continue to engage in more "conventional" activities ranging from website defacement, distributed denial of service (DDoS) attacks, and theft of personally identifiable information (PII), but they have also demonstrated a willingness to push the boundaries of their activities, which include destructive wiper malware and, potentially, cyber-enabled kinetic attacks." The escalation by Iran after key incidents by rivals is not uncommon, and is often reported on in Western news outlets. Work and Harknett's report (2) is a great overview of recent events. **Level 4**
APT 33 (aka Elfin, Magnallium, MAGNALLIUM, Refined Kitten, HOLMIUM, COBALT TRINITY) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. "Obfuscated APT33 C&Cs Used for Narrow Targeting," Feike Hacquebord, Cedric Pernet, Kenney Lu, December 10 2019.	Active since at least 2013, APT 33 carries out cyber espionage operations targeting various entities in the US, South Korea and Saudi Arabia. Nonetheless, it demonstrates special interest in infiltrating both the commercial and military sector as well as the petro-chemical production center. It is thought to work for the Iranian government. Its latest recorded attacks in 2019 comprise attacks on 50 or more organisations in Arabia Saudi, the US and other countries. For example, in July of 2019, the US discovered an attempt at introducing malware into government networks. The group also narrowly targeted a number of aviation and oil companies in the Middle East, US and Asia. **Level 3**

Document	Excerpt
APT 35 (aka Newscaster, Charming Kitten, NewsBeef, Group 83, Parastoo, Flying Kitten, Ajax Security Team, Phosphorus, IKITTENS, APT 33, ATK 35, Elfin, Magnallium, Rocket Kitten, NewsBeef, COBALT ILLUSION) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. "The Kittens Are Back in Town Charming Kitten – Campaign Against Academic Researchers," ClearSky, September 15 2019.	The Charming Kitten group is sponsored by Iran and active since at least 2014. It usually attacks the Saudi energy sector or targets likely related to it. Its latest attacks include a breach of HBO in 2017, attacks to individuals imposing sanctions on Iran as well as human right activists and journalists abroad in 2018 and targeting academics focusing their research on Iran or Iran dissidents living in the US in 2019. **Level 3**
APT (Clever Kitten) (aka Group41) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	This group targets global companies that have strategies that align with Iranian interests. Thus, it is thought that this group works under the Iranian government. It specialises in information theft and espionage and has been active since 2013. **Level 4**
APT (DNSpionage) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "DNSpionage brings out the Karkoff," Talos Intelligence, April 23 2019. (2)	The group, likely sponsored by Iran, has compromised government networks in Lebanon and the United Arab Emirates through infected websites with fake job positions. In 2019, Talos discovered ongoing activity by the group using an improved malware (Karkoff) to avoid detection. **Level 4**
APT(Domestic Kitten) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group, attributed to the Iranian government, extracts information from Kurdish and Turkish natives and ISIS supporters with Iranian citizenship through the download of malicious apps. **Level 3**
APT (Flying Kitten) (aka Ajax Security Team, Group 26) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "OPERATION "KE3CHANG": Targeted Attacks Against Ministries of Foreign Affair," FireEye, 2014. (2)	The group, first detected in 2010, has evolved from defacement to espionage operations. The group, linked to the Iranian government, is author to Operation "Saffron Rose." This was an espionage campaign against the networks of European Ministries of Foreign Affairs in the wake of the 2013 G20 meeting on the Syrian crisis. In 2015, a longstanding cyberespionage campaign against the Uyghurs was uncovered. **Level 1**
APT (Group5) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	Group5 first came to light in a malware attack against Syrian opposition in 2015. It operates from Iranian IPs and utilises Iranian-language tools **Level n/a**
APT-C-07 (aka Infy, Prince of Persia, Operation Mermaid,) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. "Prince of Persia – Ride the Lightning: Infy returns as "Foudre"," Paloalto, Tomer Bar and Simon Conant, August 1 2017.	The group, suspected to be Iran-sponsored, has targeted Iranian civil society. Its activity was first noted in 2014 and reached its height at the 2016 parliamentary elections in Iran. Though in the aftermath its activity slowed down, in 2017 a number of malware attacks were detected by Paloalto (2). The target was predominantly domestic victims and to a lesser extent actors in Iraq and the US. **Level 3**
APT (Leafminer) (aka Raspite, Sorgu, Flash Kitten) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group surfaced in 2017 and is linked to Iran. It is known for attacking government entities and businesses in the Middle East (predominantly Saudi Arabia) and in the US, East Asia and Europe to a lesser degree. **Level 3**
T-APT-14 (aka MuddyWater, Seedworm, TEMP.Zagros, Static Kitten, ATK51, Mobham, NTStats, PowerStats, TA450, COBALT ULSTER) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Recent MuddyWater-associated BlackWater campaign shows signs of new anti-detection techniques ," Talos, May 20 2019. (2)	The group is a high-profile APT and focuses on cyberespionage on Middle Eastern targets. In 2018, the group targeted governments, academy, cryptocurrency, telecommunications and the oil sectors in Oman and Lebanon. In 2019, the group targeted Kurdish political entities and organisations in Turkey. The same year, the group launched a campaign against Belarus, Turkey and Ukraine. They are also the authors of 2019 Operation "BlackWater," a campaign against Pakistan, Turkey, and Tajikistan organizations through phishing emails (2). **Level 3**

Document	Excerpt
APT 34 (aka OilRig, Helix Kitten, ATK40, Clayslide, Crambus, Helminth, IRN2, Twisted Kitten, cobalt gypsy, Chrysene, TA452, ITG13) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Hard Pass: Declining APT34's Invite to Join Their Professional Network," Matt Bromiley, Noah Klapprodt, Nick Schroeder, Jessica Rocchio, July 18 2019. (2)	The group has been active since 2014 and experts suspect this group to be tied to the Iranian government, more specifically the Iranian Intelligence agency and the Islamic Revolutionary Guard Corps (IRGC). The group is closely related to APT 33 and Elfin. Its sphere of attack is largely focused on the Middle East, specifically on financial, government, energy, chemical, and telecommunications sectors. In 2016, the group carried out an espionage campaign against Middle Eastern banks via phishing emails. In November of the same year, the group used the Disttrack malware used in the Shamoon attack to target yet another Saudi organization. In 2017, the group used fake LinkedIn Cambridge University profiles to trick victims into opening malicious documents. In December 2018, the Shamoon malware was redeployed in a third attack against various targets. This time, the malware was more destructive. A year later, a wiper attack was uncovered against energy and industrial companies in the Middle East. Finally, two of its operations were recently uncovered in 2020, one against Westat employees or US organisations contracting Westat and another one an espionage operation on the Lebanon government. **Level 3**
APT (Sima) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group, linked to the Iranian state, is known for its phishing attacks against Iranians in the diaspora. Most notably a 2016 attack on the Human Rights Watch's Emergencies Director using an email as bait. **Level 1**
APT ("Unnamed Group") "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group surfaced as a result of a leak on Iranian APTs on Telegram. Not much is known about the group other than they are sponsored by the Iranian state and are highly capable. **Level n/a**
APT (ATK120) (aka HEXANE, COBALT LYCEUM) "Hexane,"Dragos, July 8 2020.	The group is known to launch intelligence gathering campaigns against the sector related to industrial control systems in the Middle East and more broadly, the telecommunication sector in Middle East, Central Asia, and Africa. Although this group bears reported similarities to APT33 and APT34 there is no sufficient evidence to support direct affiliation to the state thereby. it is not included in the analysis. **Level n/a**
APT (Tortoiseshell) (aka Imperial Kitten) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group, linked to the Iranian state, has been active since at least 2018, using off-the-self and in-house malware to undermine IT providers in Saudi Arabia. In 2019 the group was found to be targeting US veterans searching for a job. **Level 3**
APT (Cyber fighters of Izz Ad-Din Al Qassam) (aka Fraternal Jackal, Qassam Cyber Fighters (QCF)) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	Experts have linked the group with Iran, although the hacker collective denies any association with governments and say they are operating independently. The group targets Western countries and even threatened to attack the Bank of America and New York Stock Exchange. **Level n/a**
APT (Rampant Kitten) "Rampant Kitten – An Iranian Espionage Campaign," Checkpoint research, September 18 2020.	The APT, linked to the Iranian state, is espionage- motivated. According to Checkpoint, it attacks Iranian dissidents and Iranian expats. **Level 1**
APT (Mabna Institutem) (aka Silent Librarian, COBALT DICKENS, TA407, TA4900) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. "Back to School: COBALT DICKENS Targets Universities," Secureworks, August 24 2018.	The US Treasury Department informed that this group had targeted, since 2013, 144 US universities and 176 universities in 21 foreign countries extracting around 15 billion pages of academic work. The group was also responsible for information-gathering campaigns against US Department of Labor, the US Federal Energy Regulatory Commission, and other private and non-governmental organisations. The Mabna Institute, an Iranian company and thought to be link to the Iranian state, was sanctioned by the US in relation to its suspected role in coordinating the attacks. Nonetheless, the group struck again in 2018 with a spoofing campaign on university login websites in 14 different countries. Then in 2019, the group carried out a similar attack but utilising spear-phishing tactics. **Level 1**
"Publicly Reported Iranian Cyber Actions in 2019," CSIS, 2019.	"While still not a peer with the United States or other leading cyber powers, Iran is active and skillful. Iranian hackers have probed U.S. critical infrastructure (like pipelines and dams)... Iran does not lack for sufficient cyber capability to attack U.S. targets, making the choice whether to use it a strategic calculation of benefit and risk for Iran's leaders." **Level 4**

Document	Excerpt
"Worldwide Threat Assessment of the US Intelligence Community," Daniel R. Coats, January 29 2019.	The article describes Iran's offensive cyber capabilities as increasingly refined: "Iran continues to present a cyber espionage and attack threat. Iran uses increasingly sophisticated cyber techniques to conduct espionage; it is also attempting to deploy cyberattack capabilities that would enable attacks against critical infrastructure in the United States and allied countries. Tehran also uses social media platforms to target US and allied audiences." (P. 6). This increasing sophistication signals preparation "for cyberattacks against the United States and (...)allies. It is capable of causing localized, temporary disruptive effects—such as disrupting a large company's corporate networks for days to weeks—similar to its data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017." (P. 6). **Level 3**
"The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5," Ryan C. Maness, June 1 2019.	The article lists a number of Iranian cyberattacks targeting Turkey, Israel, and Saudi Arabia. **Level 3**
APT (xHunt) (aka SectorD01, Hive0081, COBALT KATANA) "xHunt Campaign: Attacks on Kuwait Shipping and Transportation Organizations," Robert Falcone and Brittany Barbehenn, September 23 2019. (1) "xHunt Campaign: Newly Discovered Backdoors Using Deleted Email Drafts and DNS Tunneling for Command and Control," Robert Falcone, November 9 2020. (2)	The group, potentially linked to the Iranian state, targeted in 2019 a Kuwait transportation and shipping company for information- gathering purposes. In September 2020, the group breached an organisation in Kuwait, according to Palo alto. (2) **Level 3**
"Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons," US Department of the Treasury, February 13 2019.	In 2019, the Trump Administration sanctioned two entities and ten associated individuals for their support to the Iranian Revolutionary Guard Corps in their efforts to recruit and gather foreign intelligence, and attempts to install malware on US governmental and military personnel's computers. Since 2012, the US Treasury Department has issued more than 110 cyber-related sanctions against Iranian individuals and entities, oftentimes linked to branches of the Iranian government. **Level 3**
"Treasury Sanctions Iranian Organizations and Individuals Supporting Intelligence and Cyber Targeting of U.S. Persons," US Department of Treasury, February 13 2019.	In 2020, The Trump Administration sanctioned APT39, 45 associated individuals and one front company masking the Iranian government for their "years-long malware campaign that targeted Iranian dissidents, journalists, and international companies in the travel sector." Since 2012, the US Treasury Department has issued more than 110 cyber-related sanctions against Iranian individuals and entities, oftentimes linked to branches of the Iranian government. **Level 3**
"Former U.S. Counterintelligence Agent Charged With Espionage on Behalf of Iran; Four Iranians Charged With a Cyber Campaign Targeting Her Former Colleagues," US Department of Justice, February 13 2019.	In 2019 a former US counterintelligence agent was charged with espionage on behalf of Iran. At the same time, the Department of Justice charged four Iranians for attempted computer intrusion targeted against former co-workers of the charged US agent. These operations were performed on behalf of the IRGC **Level 1**
"Nine Iranians Charged With Conducting Massive Cyber Theft Campaign on Behalf of the Islamic Revolutionary Guard Corps," US Department of Justce, March 23 2018.	In 2018, the US Department of Justice charged nine Iranians for their role in massive cyber theft campaign against universities, companies and other victims. According to the indictment report, the defendants performed these intrusions on behalf of the IRGC. **Level 3**
"Cybersecurity in the Middle East and North Africa," Valentina von Finckenstein, May 2018.	"Iran started to show its capacities as early as 2000, when hacker groups with an evident relation to the Islamic Republic attacked networks of individuals, organisations and governments that were alleged to be hostile to Iran. The most prominent group linked to this collective that continues operating is the "Iranian Cyber Army", which, while it is pledging loyalty to the Supreme Leader of Iran, is not officially recognised as an entity by the government." (P. 4-5). **Level 3**
"Iran blamed for Parliament cyber-attack," BBC News, October 14 2017.	UK attribution of 2017 Westminster data breach to Iran: according to the BBC, "Whitehall officials say Iran was behind a "sustained" cyber-attack in 23 June with hackers making repeated attempts to guess passwords of 9,000 accounts" **Level 1**

Document	Excerpt
"Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities," Committee on Armed Services, United States House of Representatives, One Hundred Fifteenth Congress, First Session, March 1 2017.	The document observes about Iran: "Iran continues to see itself as a revolutionary power and this extends into cyberspace as well. Of America's adversaries, Iran has been the most persistent conducting disruptive attacks meant to disrupt US companies and infrastructure, especially banks. Fortunately, as with China, the larger improving diplomatic situation with the United States has helped to throttle back the worst offences. Since the nuclear agreement was signed, Iranian behavior is reported to be less disruptive, instead focusing on traditional political and military intelligence. Should the deal unwind, Iran would almost certainly act out using a wide range of means, including cyber disruption." **Level 3**
"Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," US Department of Justice, March 24 2016.	In 2016, the US Department of Justice indicted seven Iranian individuals for their role in a DDoS campaign lasted over 176 days. The campaign was performed on behalf of the Iranian Government, including the IRGC. **Level 3**
"Iran hacked an American casino, U.S. says," Jose Pagliery, February 27 2015.	US attribution of 2014 Sands Casino cyberattack to Iran: "Director of National Intelligence James Clapper said the Iranian government was behind a damaging cyberattack on the Sands Las Vegas Corporation in 2014. He mentioned it while testifying before the Senate Armed Services Committee" **Level 5**
"Operation Cleaver," Cylance, December 2 2014.	In addition to the infamous Shamoon attack, Iran has executed at least 44 operations dating back to 2010. Most notably, Cylance highlights "in late 2012 and early 2013 (...) Operation Ababil's Distributed Denial of Service (DDoS) attacks against US banks. These attacks were debilitating and impacted the availability of online banking services (...) FireEye's exposure of Operation Safron Rose, an espionage campaign executed by the Ajax Security Team in 2014. In May 2014 (...) a highly targeted waterhole attack that leveraged social media, dubbed Operation Newscaster (...) In June 2013, Israeli Prime Minister Benjamin Netanyahu accused Iran of carrying out "non-stop" attacks on "[Israel's] vital national systems" including "water, power and banking" . The following September of 2013, the Wall Street Journal accused Iran of hacking into unclassified U.S. Navy computers in San Diego's NMCI (Navy Marine Corp Intranet), which (...) was part of Operation Cleaver." (P.6) **Level 5**
APT (Cutting Kitten) (aka TG-2889, Threat Group 2889, ITSecTeam, Gambhar, Operation Cleaver) "Operation Cleaver," Cylance, December 2 2014. (1) "Hacker Group Creates Network of Fake LinkedIn Profiles," Securenetworks, October 7 2015. (2)	This group is author to 2012 Operation Cleaver, a large scale surveillance and infiltration campaign, affecting a range of actors worldwide: government entities, the energy, oil, gas and chemical industries, airline operators and other transportation sectors, telecommunications, defence, tech firms and universities. Cutting Kitten is likely linked to Threat Group 2889, both attributed to Iranian entities. The most recent operations include an attack on a New York City Dam in 2013 and a 2016 social engineering attempt on LinkedIn to infect victim's computers through fake resumes. **Level 3**
"In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," Nicole Perlroth, October 23 2012.	US attribution of 2012 Saudi Aramco and RasGas compromise to Iran: according to a New York Times article, "United States intelligence officials say the attack's real perpetrator was Iran, although they offered no specific evidence to support that claim". **Level 5**
"In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," Nicole Perlroth, October 23 2012. (1) "We, behalf of an anti-oppression hacker group," Pastebin, August 15 2012. (2) "ICS Joint Security Awareness Report (JSAR-12-241-01B): Shamoon/DistTrack Malware (Update B)," Cybersecurity & Infrastructure Security Agency, October 16 2012.(3)	APT 33 employed Shamoon malware to wipe out or destroy around 30,000 Saudi oil company Aramco's computers. An anti-oppression hacker group labeled "Cutting Sword of Justice" claimed responsibility for the attack, taking a stance against the Al-Saud regime (2). However, US intelligence services have attributed the attack to Iran: "Iranian nation-state actors have been observed deploying Shamoon malware against industrial control systems." (3). **Level 5**
"Iran blamed for cyberattacks on U.S. banks and companies," Ellen Nakashima, September 21 2012.	US attribution of 2012 Operation Ababil to Iran: According to a Washington Post article, Senator Joseph Liberman, Charmain of the Homeland Security and Governmental Affairs Committee at the time of the attack, said "I don't believe these were just hackers who were skilled enough to cause disruption of the Web sites. I think this was done by Iran and the Quds Force, which has its own developing cyberattack capability". The article further mentions that US officials have also attributed the attack to the Iranian government. **Level 3**

Israel

Cyber Transparency Score Untransparent

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■■■■

Organization for Offensive Cyber (1952)
Unit 8200 - Joint Cyber Defense Division (JCDD) of the Israel Defense Forces

National Cyber Power Index (2020)
Ranked 6th when it comes to offense

National Cybersecurity Index (2022)	67.53 (34th)
Internet Penetration (2020)	90%
Internet Freedom Score	n/a

Transparency Description

A lack of transparency is observed for Israel. While Israeli strategies overtly identify cyberspace as a domain of war and refer to the deployment and use of "active efforts" against adversaries who undermine Israeli interests, to date, official documents do not go beyond the mere acknowledgement of offensive capabilities, and no military doctrines nor core principles of engagement have been disclosed. Nevertheless, Israel is largely perceived as to possess one of the most advanced military cyber capabilities in the world, and willing to use those capabilities to achieve strategic objectives. Strategic objectives are known to be implemented by at least two organisations, namely the C4I Directorate, for defence operations, and the Unit 8200, for offensive operations. Indeed, several offensive cyber operations against regional adversaries – ranging from intelligence and strategic cyber operations (e.g. *Stuxnet*, *Flame*, *Duqu*) to tactical cyber and electromagnetic activities (e.g. *Operation Orchard*) - have been routinely attributed to Israel.

Declared Capability Rating

Score ■■■□□

Israel mentions offensive cyber capabilities in its national strategy and has published several cyber strategies to date. Its disclosure does not go beyond the mere acknowledgement of their offensive capability. The (civilian) National Cybersecurity Strategy of 2017, lays out the defensive and offensive capabilities of the IDF in limited detail and with flexible leadership and oversight between the Israeli Defence Forces (IFD) and the Israel National Cyber Directorate under the Prime-Minister's office.

Data availability rating (1 being highest number of sources, 10 lowest): **5/10**

Document	Excerpt
"Fighting in five dimensions: cyber and spectrum targets gained operational legitimacy in "guardian of the walls," Israel Defense, May 25 2021.	In an interview with a former official, it is reported that "For the first time in the world's books of warfare, cyber fighting took place in Gaza. This is about digitising the IDF in the face of Hamas counter-warfare. As head of the ICT division, you need to produce targets for destruction. It's a new fighting dimension" Level 1
"Israel International Cyber Strategy," Israel National Cyber Directorate, April, 2021.	The strategy refers to the use of cyber tools in the interest of national security domestically and abroad: "cyber tools may be deployed as appropriate against cyber adversaries who undermine Israeli interests. These are designed to intercept, defend against, and deter adversaries beyond Israeli borders when needed, in accordance with domestic and international law." (P.7) Level 3

Document	Excerpt
"Israel National Cyber Security Strategy," National Cyber Directorate, 2017	The strategy includes enhancing deterrence as a means to campaign against attackers (P.12) while also reiterating active efforts against threats: "National defense campaigns incorporate defensive effort, to contain such attacks and their ramifications together with active efforts to confront the sources of the threats." (P.12) **Level 3**
"Deterring Terror: How Israel Confronts the Next. English Translation of the Official Strategy," Belfer Centre, 2016.	The strategy acknowledges cyberspace as another domain of war: "Cyberspace is another area of combat. Defense, intelligence collection, and assault activities will be carried out in this space" (P.44) and goes on to indicate the role of cyber in traditional warfare: "Cyber effort within the framework of a War or Emergency situation will support the defensive and offensive efforts at all levels of fighting — strategic, operative, and tactical." (P.21) **Level 3**
"Israel Defense Forces Strategy Document," IDF Chief of General Staff Lt. Gen. Gadi Eizenkot, August 2015.	Cyber is included in the means of war. The document states: "[Conditions of 'Victory and Defeat']: Maintain the continuity of the economic and war efforts through effective and multi-dimensional defense (land, sea, air, cyber)." Cyber is described within the ambit of war as an additional means of warfare: "Cyber effort within the framework of a War or Emergency situation will support the defensive and offensive efforts at all levels of fighting - strategic, operative, and tactical." It reiterates that: "Cyberspace is another area of combat. Defense, intelligence collection, and assault activities will be carried out in this space" And provides further detail: "Building the IDF's force in this sphere will be based on these actions: Establish a cyber arm that will constitute the main HQ subordinate to the Chief of the General Staff to operate and build the IDF's cyber capabilities and will be responsible for planning and implementing combat in cyberspace." **Level 3**
"Barak Acknowledges Israel's Cyber Offensive for First Time," Gili Cohen and Oded Yaron, Haaretz, June 6 2012.	Defence Minister Ehud Barak acknowledged Israeli's offensive cyber operations. **Level 2**

Perceived Capability Rating

Score ■■■■■

Israel is perceived as having developed advanced offensive cyber capabilities that are integrated within its overall military structure, and to having the intent to use those capabilities to achieve strategic objectives, which has been demonstrated by the numerous offensive cyber operations that have been attributed to Israel. These range from intelligence and strategic cyber operations (e.g. Stuxnet, Flame, Duqu) to tactical cyber and electromagnetic activities (e.g. Operation Orchard). These operations are mostly directed at regional adversaries and often carried out by Unit 8200. To this end, Israel is perceived to work closely with its Western allies, most notably the US. Finally, the strong Israeli cybersecurity industry base is considered to be of significant added value to the military, and has been found to export spyware capabilities to foreign governments.

Data availability rating (1 being highest number of sources, 21 lowest): **6/21**

Document	Excerpt
"Iran says Israel, U.S. likely behind cyberattack on gas stations," Reuters, October 30 2021.	"Iran's civil defence chief on Saturday accused Israel and the United States of being the likely culprits behind a cyberattack which disrupted gasoline sales across the Islamic Republic, but said a technical investigation was yet to be completed: "We are still unable to say forensically, but analytically I believe it was carried out by the Zionist Regime, the Americans and their agents," Gholamreza Jalali, head of civil defence which is in charge of cyber security, told state TV in an interview." **Level 3**
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	The index ranked Israel in 6th place in the offense metric.
"Israel's National Cybersecurity and Cyberdefense Posture," Center for Security Studies, 2020	The report mentions Unit 8200 as *de facto* carrying out offensive cyber operations: "Intelligence and offensive cyber capabilities are also applied to support the conventional military sector." **Level 5**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Unit 8200's core mandate is defensive (textually), but the authors (and most other observers) claim that it uses offensive tools pre-emptively. It employs between 5.000 and 10.000 people (P. 10). The report lists a number of offensive cyber operations that can be attributed to Unit 8200, and some that are likely committed by Unit 8200 (P. 9). Unit 8200 also frequently collaborates with its peers, including the US, Canada, and Britain (P. 9-10). Having this into account, the report draws the conclusion that "its size and the sophistication of some of its operations – e.g. Stuxnet, which used four zero-day vulnerabilities – one can assume that it possesses substantial financial resources." (P. 16). **Level 5**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	The Stuxnet Virus (2005–2010) was allegedly partly attributed to Unit 8200: "The virus successfully disabled the nuclear centrifuges in Natanz. According to some accounts, the virus was part of the joint Operation Olympic Games between the United States' NSA and Israel's Unit 8200" (P.9) **Level 5**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Operation Orchard (September 2007) was attributed to Unit 8200: "Unit 8200 most probably jammed Syrian radar systems without alerting air defense operators in order to allow for a precise airstrike against a Syrian nuclear facility in Deir ez-Zor...Unit 8200 conducted SIGINT to locate the facility and caused the anti-aircraft defense to malfunction during the attack, leveraging electronic sabotage" (P.9). This was a CEMA (Cyber and Electromagnetic Activities) operation and it was used to support another military operation, in this case the airstrike against the Syrian nuclear facility. **Level 5**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Operation Full Disclosure (March 2014) was attributed to Unit 8200. The operation consisted of an "Israeli commando intercepted an Iranian ship in the Red Sea, which carried military arms and equipment destined for Hamas. The operation was made possible by the Unit's intelligence obtained through "advanced cyber and communications capabilities" (BBC News, 2014; Dombe, 2014)." (P.9) **Level 1**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	The Ogero Incident (May 2017) was attributed to Unit 8200: the "Lebanese government blamed Israel of having launched a sophisticated cyberattack on the state's telecommunications company Ogero to spread disinformation through audio messages to over 10,000 Lebanese citizens, namely that Hezbollah's leader was behind the death of the group's top military commander" (P.9) **Level 3**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Operation Flame (2007–2012), likely attributed to Unit 8200, was " a sophisticated multi-functional modular malware apparently produced by a sophisticated team for the purposes of cyberespionage. The targets spanned across Iran, Israel and the Palestinian territories. According to an ArsTechnica article...the malware also allegedly infected some Iranian oil facilities. It reportedly also shared similarities (i.e. a common plugin) with an earlier version of Stuxnet." (P.9) **Level 5**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Operation Duqu (2009–2011), likely linked to Unit 8200, "was another complex, multi-stage malware that targeted industrial systems manufacturers in over twelve countries, including Iran and Sudan but also Hungary. According to Kaspersky, the malware shared a common development platform, the "Tilded" framework, with Stuxnet" (P.9) **Level 5**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Operation Gauss (2011–2012), likely executed by Unit 8200, "was a cyberespionage toolkit made for stealing system information and sensitive data. It affected thousands of victims, most of them located in Lebanon, Israel and Palestine. The malware exploited the same vulnerability as Stuxnet and Flame" (P.9) **Level 1**

Document	Excerpt
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Operation miniFlame (2012), likely attributed to Unit 8200, "was a sophisticated cyberespionage malware targeting fewer than one hundred machines in Lebanon, Iran, Kuwait, Qatar and the Palestinian Territories. Its backdoor was identified to be one of four malware clients that communicated on the same C2 protocol as Flame. According to Kaspersky, it operated as a previously unknown module in Flame and Gauss" (P.9) **Level 5**
"The Israeli Unit 8200 An OSINT-based study," CSS ETH Zurich, December 2019.	Operation Duqu 2.0 (2014–2015), a variant of Duqu, is likely linked to Unit 8200 and consisted of "a sophisticated cyberespionage malware operation that targeted organizations and venues linked to the P5+1 Iran Nuclear Agreement negotiations in Vienna and Switzerland (Kaspersky Lab, 2015). According to an article by The Guardian, the sophistication and context of the malware strongly ties it to Israel" (P.9) **Level 5**
"Israel eases rules on cyber weapons exports despite criticism," Tova Cohen and Ari Rabinovitch, August 22 2019.	One thing that should be mentioned about Israeli cyber capabilities is that their private sector is often accused of selling spyware and other means, mainly focused on espionage, to other states (i.e. see the Ethiopia section). This article details the level of complacency by the Israeli government in allowing this to happen, and the outcry from various international organizations/actors against it. **Level 2**
"Cybersecurity in the Middle East and North Africa," Valentina von Finckenstein, May 2018.	According to the article, "For the leading cyber power [in the MENA region] Israel, and particularly for the present administration, the development of cyber capabilities is one of the state's highest national security priorities," (P. 4). As such, "The Israeli government's cybersecurity institution, the National Cyber Directorate ... reached a budget of $500 million in 2018. The country accounts now for the second-largest number of cybersecurity deals globally after the U.S." (P. 4). **Level 5**
APT (Duqu Group) (aka Unit 8200 Central Collection Unit of the Intelligence Corps, Israeli SIGINT National Unit (ISNU) "Spy virus linked to Israel targeted hotels used for Iran nuclear talks; cybersecurity firm Kaspersky lab finds three hotels that hosted Iran talks were targeted by a virus believed used by Israeli spies," Entous, A., & Yadron, June 10 2015. (1) "The Duqu 2.0," Kapersky, June 11 2015. (2)	This APT, first uncovered by Kapersky Lab in 2011, is thought to originate from Unit 8200, an Israeli Intelligence Corps unit. In 2011, a spear phishing attack was launched by this group. In 2014, a campaign with the same techniques compromised international organizations. In 2015, Kapersky reported on an espionage-campaign carried out on hotel networks "hosting high-stakes negotiations between Iran and world powers over curtailing Tehran's nuclear program." (1) Although this new virus was not directly linked to Israel, the virus infecting the hotel systems bore great resemblance to the one from the 2011 and 2014 attacks. This virus was sophisticated and difficult to replicate, suggesting that whoever carried out the attack had to have had access to the original malicious code. **Level 5**
"The Real Story of Stuxnet," David Kushner, February 26 2013.	"Although the authors of Stuxnet haven't been officially identified, the size and sophistication of the worm have led experts to believe that it could have been created only with the sponsorship of a nation-state, and although no one's owned up to it, leaks to the press from officials in the United States and Israel strongly suggest that those two countries did the deed." **Level 4**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	CSIS explains how Unit 8200 handles attacks: "Military-oriented operations are split between the Israel Defence Forces' Unit 8200—which deals with signals intelligence and encryption—and the C4I Corps." (P. 31) **Level 4**
"Iran blames U.S., Israel for Stuxnet malware," CBS News, April 16 2011.	Iranian attribution of 2010 Stuxnet cyberattack to the US and Israel: "A senior Iranian military official says experts have determined the United States and Israel were behind a mysterious computer worm known as Stuxnet that has harmed Iran's nuclear program" **Level 5**

Italy

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber (2020)	Joint Command for Network Operations (Comando per le Operazioni in Rete) (MoD)
National Cyber Power Index (2020)	Ranked 29th overall
National Cybersecurity Index (2022)	79.22 (20th)
Internet Penetration (2020)	70%
Internet Freedom Score	76/100 (Free)

Transparency Description

Italy has declared to be in possession of offensive cyber capabilities and disclosed which organisations are in charge of carrying out cyber operations. The Strategic Concept published in 2020 by the Chief of Defence Staff highlighted the establishment of the Joint Command for Network Operations, which is responsible for planning, conducting, and implementing the entire range of military operation in the cyber domain to counter and neutralise potential threats to networks, systems, and services of the Defence. However, such capabilities appear to be mostly under development. No detail has ever been disclosed ad very few documents released after the years 2016-2017 refer to the progresses achieved in developing offensive cyber power. In light of the purely aspirational nature of current disclosures and due to strict legal mandates, Italian cyber capabilities are not perceived as highly developed. It has been reported that Italy, similarly to other countries, is planning to structure a cyber command. However, it is still unclear if and to what extent a dedicated unit has already been established.

Declared Capability Rating

Score

Italy has disclosed that it has an offensive cyber capability and the organizations in charge, albeit mostly referred to as a capability being under development. Details about their offensive capability were not disclosed in the analysed documents.

Data availability rating (1 being highest number of sources, 10 lowest): **5/10**

Document	Excerpt
"National Cyber Strategy Implementation Plan", Presidency of the Council of Ministers, May 2022	The Implementation Plan sets out all the measures necessary to fully implement the goals set out in the National Cyber Strategy. Among such measures, the document highlights the need to enhance the capabilities to attribute and respond to malicious cyber operations. [Original: "Measure #40. Rafforzare I meccanismi nazionali volti all-applicazione degli strumenti di deterrenza definiti a livello europeo e internazionale per la risposta ad attacchi cyber. In tale contest, si pone l'esigenza di definire un documento sul posizionamento e sulla procedura nazionale in materia di attribuzione."] Level 3
"National Cyber Strategy 2022-2026", Presidency of the Council of Ministers, May 2022	The Strategy is mostly focused on cyber resilience. However, it makes reference to the integration of cyber capabilities within the military, as well as to the aspiration to further develop cyber capabilities to enhance national security [Original: "...il Ministero della Difesa definisce e coordina la politica militare, la governance e le capacita' militari nell'ambiente cibernetico, nonche' lo sviluppo di capacita' cibernetiche...] (p. 08) The document underscores the need to adopt an "active defence" posture to deter malicious actors. [Originale: "A seguito dell'esperienza maturate dal nostro Paese...e'apparso chiaro come sia necessario puntare su tattiche di difesa attiva – che si aggiungono alle buone pratiche di cyber resilienza e due diligence – volte ad aumentare I costi di eventuali attivita' cyber offensive, cosi' da renderle economicamente svantaggiose."] (p. 11) Level 3

Document	Excerpt
"National Cybersecurity Agency", Presidency of the Council of Ministers, 2021	Law Decree 82/2021 established the National Cybersecurity Agency (CAN), tasked with strengthening national cybersecurity and resilience posture, as well as adopting a whole-of-society approach to cyber defence. No stated offensive cyber capability. **Level 0**
"Concetto Strategico del Capo di Stato Maggiore della Difesa", Ministry of Defence, 2020	The Strategic Concept published by the Chief of the Defence Staff highlights the establishment of the Joint Command for Network Operations (COR), resulting from the integration of the CIOC and C4 Defence unit. The COR is structured in three Divisions (C4, Security and Cyber Defence, Cyber Operations), and is tasked with planning, preparing, and conducting cyber operations through dedicated cells (COC) against any possible threat or action to Defence networks, systems, and IT services, both at home and in the Theatre of Operation. **Level 3**
"Ecco come ci occupiamo della cyber-difesa nazionale. Parla il generale Vestito," Stefano Pioppi, May 30 2018.	The interview with the commander of the Joint Command for Cyber Operations (CIOC) reveals that the command is in the process of building the technological capabilities that will allow the CIOC to conduct cyber operations. The commander informs that the command has been given substantial resources for the development of capabilities. For instance, the command employs a few hundred people but is planning on doubling that amount in the near future. When referring to cyberattacks, the commander simply states that there is no authorisation in the domestic legal system and in international law to carry out offensive attacks. **Level 2**
"The Italian Cyber Defence Build Up," Francesco Vestito, May 3 2018.	The CIOC will be "responsible for planning and conducting "Cyber Operations" to support military operations both in Italy and, if required, outside the national borders." **Level 3**
"Cybersicurezza, a cosa serve il Cioc ? Risponde Alfano (non Angelino)," Public Policy, April 18 2017.	The article describes the competencies of the Joint Cyber Operations Command (JCOC): "Make a contribution to national security, in particular with respect to the risk of cyberattacks, and at the same time plan operations in support of military action"(...) "The Command – explained Alfano [Undersecretary of Defence] – will be engaged on a double front: on the one hand, to guarantee its contribution to national security, strengthening the capabilities of defence against cyber-attacks, on the other hand to develop the planning and conducting capabilities of 'computer network operations' (CNO) in support of military operations both in Italy and outside national borders" [Original: Dare un contributo alla sicurezza nazionale, in particolare rispetto al rischio di attacchi informatici, e al contempo pianificare operazioni a supporto dell'azione militare (...)"Il Comando – ha spiegato Alfano – sarà impegnato su un duplice fronte: da un lato, garantire il proprio contributo alla sicurezza nazionale, potenziando le capacità di difesa da attacchi cibernetici, dall'altro sviluppare le capacità di pianificazione e conduzione di 'computer network operations' (Cno) a ormati delle operazioni militari sia in Italia, che al di fuori dei ormati nazionali."] **Level 3**
"Reparti," Ministry of Defence, 2015.	According to the Ministry of Defence, the Security and Cyber Defence Department (Reparto Sicurezza e Cyber Defence) "ensures the management of the correct security posture and the effective level of protection from cyber threats (*Cyber Defence*) of the ICT infrastructures of the Joint Summit areas, developing, for the area of competence, activities aimed at identifying and evaluating new security capabilities and their inclusion in the network architecture, the continuous monitoring of the *cyber* situation and the management of IT security incidents, the verification of vulnerabilities and the development of prevention strategies" and the Cyber Operations Department [Reparto Operazioni Cibernetiche]"is responsible for planning, conducting and implementing the entire range of military operations in the cyber domain to counter and neutralise any possible threat and / or adversary action brought to the networks, systems and services of the Defence, both on the national territory and in the Operational Theatres. In this context, it also takes care of personnel training, supports doctrinal development, and provides advice for the innovation and *procurement* of Defence in the *cyber* field." **Level 0**
"White Paper for International Security and Defense," Ministry of Defence, July 2015.	The document notes the emergence of cyberspace as a fifth domain of war and expresses the necessity to develop defensive capabilities: "specific defensive operational capabilities must be dedicated to these areas [cybernetic], in order to preserve the safety of the "national system" and increase the solidity of the political, economic, and social structures" "(P.49). It also mentions the existence of the Cybernetic Operations Command. **Level 0**
"National Strategic Framework for Cyberspace Security," Presidency of the Council of Ministers, December 2013.	The framework describes the objective to set up "An effective institutional communication of national dissuasion and deterrence capabilities in cyberspace may work as a disincentive to potential adversaries and criminals." (P. 25) In addition, the Ministry of Defence "Plans, executes and sustains Computer Network Operations (CNO) in the cyber domain in order to prevent, localise, defend (actively and in-depth), oppose and neutralise all threats and/or hostile actions in the cyber domain targeting ICT networks. **Level 3**

Perceived Capability Rating

Score ■■□□□

Italian offensive cyber capability, as indicated in recent indexes, is perceived to be mostly under development and constrained by limited legal mandates.

Data availability rating (1 being highest number of sources, 21 lowest): **12/21**

Document	Excerpt
« L'Italia e la difesa cibernetica, » Istituto Affari Internazionali, September 2021	The report highlights the "impossibility to carry out offensive operations" for Italy, given the lack of offensive capabilities and supporting legal structures Level 0
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Italy is ranked low for offense capabilities. It is ranked 29th out of 30 in the overall ranking, only coming after Egypt. Level n/a
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	It notes the limitations of Italy in the development of its capabilities: "Despite ... plans in some of these countries (e.g. Italy and Poland) to establish a command ... it remains unclear to what extent the entities are operational or are capable to conduct offensive cyber operations." (P. 187). Level 2
"Le operazioni militari nel dominio cibernetico e le attività di intelligence," Claudio Catalano, October 2019.	"According to current legislation in Italy, in the absence of a clear legal framework (as it is not possible to automatically and permanently extend the interpretation of the functional guarantees of the art.17 paragraph 7 of Law no. 124/2007 to the cyber operations of the Afs) the Afs should refrain in peacetime from any kind of OCO, including the penetration of third party networks, in the absence of parliamentary authorisation and specific legislation." [Original: In base alla vigente normativa in Italia, in assenza di un quadro giuridico chiaro, non essendo possible estendere per via interpretativa in modo automatic e permanente le garanzie funzionali di cui all'articolo 17, comma 7 della Legge n. 124/2007 alle operazioni cibernetiche condotte dalle Forze Armate, queste ultime dovrebbero astenersi dal compiere qualsiasi tipo di operazione cibernetica offensiva, inclusa la penetrazione delle reti di terzi, in assenza di autorizzazione parlamentare e di normative specifica.] However there is some possible leeway, for instance, "the 2017 "National Plan for Cyber Protection and Information Security" in the objective on "1.4 Development of Core Operational Capabilities Suitable for Carrying Out Defence Tasks in the Cyber Environment" supports the development of commands capable of planning and conducting military operations in cyberspace" [Original: Il "Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica" del 2017 nell'obiettivo sullo "1.4 Sviluppo delle capacità operative fondamentali, idonee ad espletare i compiti della Difesa nell'ambiente cibernetico" sostiene lo sviluppo di comandi in grado di pianificare e condurre operazioni militari nello spazio cibernetico.] Moreover, the Armed Forces could support cyber operations by the intelligence services but solely in conflict situations. Nonetheless, the national legislator has continued the demilitarisation of the intelligence services in accordance with 124/2007 (P.93). Level 1
"Cyber defence: entro fine anno comincerà ad operare il comando operazioni cibernetiche," Ebe Pierini, July 23 2017.	The article notes Italy's efforts to enhance "cyber defence" to catch up with other countries that have already developed offensive capabilities. Within the Joint Command for Cyber Operations (Comando Interforze per le Operazioni Cibernetiche), the article notes there is plans to create "cybernetic operational cells (...) that will be responsible for conducting cyber defense and cyberattack operations." Original : Verranno poi formate delle cellule operative cibernetiche che saranno deputate a condurre operazioni di cyber difesa e di cyber attacco.] Level 1
"EMSO, the great value of using the electromagnetic spectrum as a response to current threats," Luca Tattarelli, June 16 2017.	The article mentions the importance of focusing attention on "the management of the electromagnetic spectrum, with the aim of integrating modern Cyber, Electronic Warfare, Signal Intelligence (Sigint) and frequency management capabilities." According to the Chief of Defence Staff General Claudio Graziano in the current climate, "60% of our activity is cyber." In fact, he mentions that "The Joint Force Command is already operating and will reach full capacity in 2019." Level 2
"Ecco come l'Italia vuole proteggersi dai cyberattacchi," Carola Frediani, January 20 2017.	The article explains "it is likely that the Joint Command for Cyber Operations will also deal with a topic that is still little debated and thorny: the development of offensive capabilities" [...] it "will take care of supporting and protecting military operations, but it should also act as a coordination between the armed forces and other national structures that deal with the cyber protection of the country." Level 2

Document	Excerpt
"Italy Cyber Readiness at a Glance," Melissa Hathaway Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri, November 2016.	Describes that, how in accordance with other NATO members, the Italian Ministry of Defence has "acknowledged that cyberspace is now the fifth domain of warfare." (P. 22). They have also announced plans for some new cyber centers, which may deal with offensive attacks. The authors write: "[Italy] will develop a Computer Network Operations (CNO) unit with planning and management capabilities in support of military operations within Italy and abroad." (P. 22). Moreover, Italy also participates in numerous international cyber trainings and such. (P. 23). Thus, overall, it appears that Italy has been lagging behind on cyber defence for a while, and similarly on any offensive cyber capabilities. **Level 2**
"Italy Cyber Readiness at a Glance," Melissa Hathaway Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri, November 2016.	The paper describes that, in accordance with other NATO members, the Italian Ministry of Defence has "acknowledged that cyberspace is now the fifth domain of warfare." (P. 22). They also announced plans for some new cyber centres, which may deal with offensive attacks. The authors write: "[Italy] will develop a Computer Network Operations (CNO) unit with planning and management capabilities in support of military operations within Italy and abroad." (P. 22). Italy also participates in numerous international cyber trainings and such. (P. 23). Overall, it appears that Italy has been lagging behind on cyber defence for a while, and similarly on any offensive cyber capabilities. **Level 2**
"Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014.	In one instance, Italy was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	States that "The Italian military has an electronic warfare unit responsible for intelligence, surveillance, target acquisition, and reconnaissance," (P. 32). It also mentions how Italy has been part of numerous international initiatives on cyber security. **Level 2**

Japan

Cyber Transparency Score Transparent and Low Capability

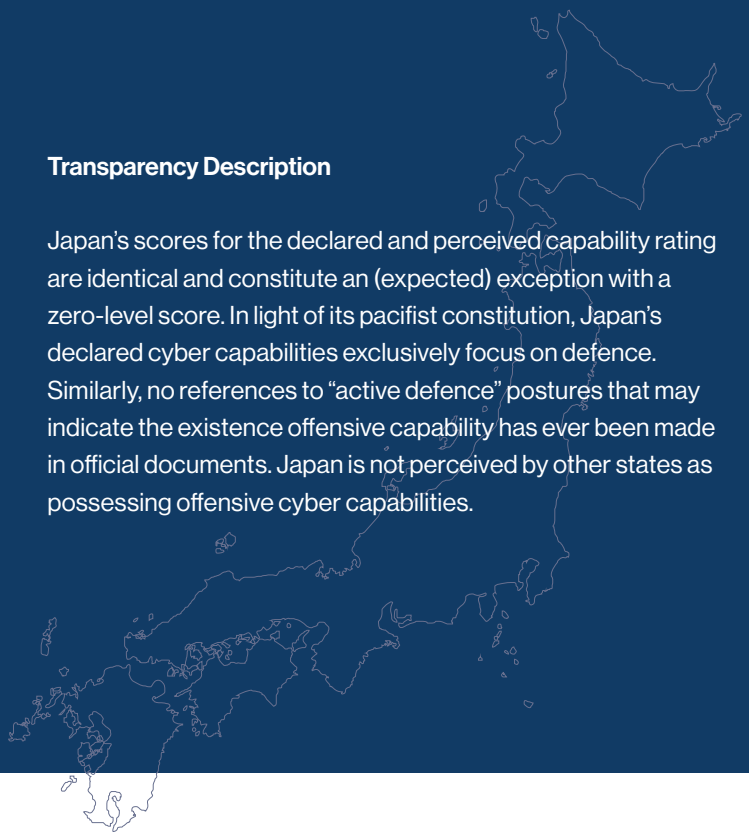
Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ☐☐☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	21.03 (9th)
National Cybersecurity Index (2022)	63.64 (44th)
Internet Penetration (2020)	90%
Internet Freedom Score	76/100 (Free)

Transparency Description

Japan's scores for the declared and perceived capability rating are identical and constitute an (expected) exception with a zero-level score. In light of its pacifist constitution, Japan's declared cyber capabilities exclusively focus on defence. Similarly, no references to "active defence" postures that may indicate the existence offensive capability has ever been made in official documents. Japan is not perceived by other states as possessing offensive cyber capabilities.



Declared Capability Rating

Score ☐☐☐☐☐

No official disclosure of offensive capabilities or aspirations were found for Japan, which can be explained by its pacifist constitution. Instead, defensive capabilities are emphasised and any future capability that would considered as offensive in the broadest sense is likely to be considered as defensive-reactive.

Data availability rating (1 being highest number of sources, 10 lowest): **5/10**

Document	Excerpt
"Defense of Japan," Ministry of Defense, 2020.	The white paper does not directly mention offensive cyber capabilities. It only refers to "Neutralising use of electromagnetic spectrum, including radar and communications of an opponent who intends to invade Japan" (P.274) Level 0
"Medium Term Defense Program (FY 2019 - FY 2023)," December 2018.	No mention of offensive cyber capabilities or intentions is made, although the programme emphasises the need to create additional cyber units within the ground forces. Level 0
"National Defense Program Guidelines for FY 2019 and beyond," December 2018.	While the document defines cyberspace as a warfare domain, there is no reference to the development of offensive capabilities. Level 0
"Cybersecurity Strategy," National Center of Incident Readiness and Strategy for Cybersecurity, July 27, 2018.	No mention of offensive cyber capabilities or intentions is made. Level 0
"Cybersecurity Strategy," September 2015.	The emphasis is on defensive rather than offensive capabilities, there is no mention of aspiring to build offensive cyber capabilities. Level 0

Perceived Capability Rating

Score ☐☐☐☐☐

No existing or aspiring offensive cyber capability was perceived for Japan. Although it is recognised to – in theory – have the ability to develop a strong capability, most observers have yet to observe this in practice, which is mostly attributed to its restrictive Self-Defence Forces Law

Data availability rating (1 being highest number of sources, 21 lowest): **14/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Japan is ranked 9th overall and ranked 16th in terms of cyber offence.
"Japan and cyber capabilities: how much is enough?" Franz-Stefan Grady and Yuka Koshino, August 28 2020.	Japan is increasing their investment in cyber defence, and also the amount of their forces (from 220 to 290 by the end of March 2021). The article mentions some challenges with regards to the nation's strategy if "JSDF plans to move towards a limited offensive cyber posture in the event of an 'armed attack'" this " would require a revision to Japan's Self-Defence Forces Law to clarify whether cyber responses fall under the category of 'use of force' or 'use of weapons' for a defence operation, or for a public security operation" because "Without revision, Japan would face legal difficulties in using some of the capabilities included in the new defence strategy." **Level 0**
"The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5," Ryan C. Maness, June 1 2019.	The paper details several incidents where Japan was allegedly behind cyber operations on South Korea. Many of these incidents were part of an ongoing string of DDoS attacks and such between South Korea and Japan on their commemoration day, or about disputed islands. It is not entirely sure if these incidents were government sponsored or by individual hackers. As a result, this remains a level 0. **Level 0**
"Japan: The Reluctant Cyberpower," Franz-Stefan Gady, March 2017.	In a different report, the same author predicts that Japanese development of offensive capabilities is currently not likely but could change, stating: "The Abe administration has been careful not to abandon the JSDF's defensive posture in cyberspace, and has not indicated that is willing to develop offensive cyberwar capabilities. This, however, may change should the new US administration abandon the United States' historic solid defence commitment to Japan." (P. 28). **Level 0**
"Japan's Defense Ministry Plans to Boost Number of Cyber Warriors," Franz-Stefan Gady, July 17 2017.	According to the document, Japan was apparently planning to increase cyber capabilities. The document explains that Japan does not officially have offensive cyber capabilities, as it violates their neutrality policy. Instead, they rely on the US: "Japan relies on the U.S.-Japan alliance to increase its cyberwarfare capabilities, however, cooperation between the two countries remains underdeveloped. The U.S.-Japan Treaty of Mutual Cooperation and Security also does not offer concrete guidelines whether a cyberattack on Japanese critical information infrastructure mandates U.S. military intervention in cyberspace." **Level 0**
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	The report notes that the Japanese Cyber Defence Unit only employs 90 individuals (P. 45). It further notes Japanese-American collaborations in military uses of cyber, though not expressly in offence. The document concludes by stating: "Japan would benefit from a more defined doctrine or strategy outlining how cyberspace is used in warfare and a more developed approach to protecting its defence industry." (P. 45). **Level 0**
"U.S.-Japan Cooperation in Cybersecurity," James Andres Lewis, November 2015.	This document mirrors what the previous source says: The US, in theory, does the offensive work for Japan. It adds on that "Japan could acquire cyber attack capabilities under the current interpretation of the constitution, since attack capabilities play an increasingly important role in cyber defense and can be limited to defensive purposes." (P. 2). **Level 0**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	The CSIS notes that "The Command's Cyberspace Defence Unit will integrate cyber defence into the military, provide coordination and technical and training assistance, and research cyberwarfare options." (P. 33). **Level 0**

Kazakhstan

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■◧☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	48.05 (70th)
Internet Penetration (2020)	86%
Internet Freedom Score	33/100 (Not free)

Transparency Description

Kazakhstan's scores for the declared and perceived capability rating differ considerably at the lower-end of the spectrum. It has never publicly declared to be in possession of offensive cyber capabilities. From the outside, Kazakhstan is perceived as using commercial spyware tools acquired from foreign vendors to carry out man-in-the-middle attacks for domestic surveillance purposes.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■◧☐☐☐

Kazakhstan's offensive cyber capability appears to be mostly limited to spyware acquired from foreign vendors and man-in-the-middle attacks for domestic surveillance purposes. Kazakh participation in CSTO military (cyber) exercises was noted, but the role of offensive capabilities in these exercises remains unclear.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"Kazakhstan government is intercepting HTTPS traffic in its capital," Catalin Cimpanu, December 6 2020.	The Kazakhstan government attempted to force its citizens to download a digital certificate on their devices to access sites such as Google, Twitter, YouTube, Facebook, Instagram, and Netflix. The installation of the certificate on the user's device would allow the government to intercept all of their online activity. The government declared their actions were part of a cybersecurity exercise. This is the third attempt by the government to gain control of its population's internet activity. Level 1

Document	Excerpt
"Extensive hacking operation discovered in Kazakhstan," Catalin Cimpanu, November 23 2019.	Identifies one offensive cyber operation sponsored by the Kazakh government: a 2016 espionage attack against government dissidents. The software used was made by the Israeli company NSO Group, and has been used by numerous other nations. **Level 1**
"The shadow hovering over Central Asia-Golden Eagle (APT-C-34) organized an attack to expose," 360 Core Security Technology Blog, November 20, 2019.	"In 2015, after HackingTeam was attacked and leaked data, Kazakhstan's national intelligence agency was confirmed to have purchased HackingTeam software and had an official email with HackingTeam to seek technical support for cyber weapons." **Level 1**
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	Kazakhstan has acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
"Armenia to Participate in Kazakhstan CSTO Drills," Joe Peerson, August 12 2014.	"Three thousand soldiers from six countries will take part in psychological and cyber warfare exercises when they meet for combat maneuvers in Kazakhstan on August 18 to 22, Aysor reports. The armed forces are gathering for the first time to participate in war games under the Collective Security Treaty Organisation (CSTO), which unites Rapid Reaction Force units from Armenia, Belarus, Kazakhstan, Kyrgyzstan, Russia and Tajikistan." **Level 1.5**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	"Kazakhstan's 2011 Military Doctrine identifies cyberterrorism and the use of information technologies and psychological warfare to interfere in Kazakhstan's internal affairs as threats facing the country." (P. 34) **Level 1**

Lebanon

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	n/a
Internet Penetration (2020)	84%
Internet Freedom Score	51/100 (Partly free)

Transparency Description

Lebanon scores for the declared and perceived capability rating differ considerably at the lower-end of the spectrum. Lebanon has not officially declared to be in possession of offensive cyber capabilities and it is currently perceived as mostly using surveillance tools to carry out espionage operations. In this regard, sources reported that APT Dark Caracal, which has exfiltrated significant data related to IP and PII in at least 21 countries, could be affiliated with the Lebanese government. Other sources also link APT "Volatile Cedar", which targeted companies from the US, UK, Egypt, Israel, to the Lebanese government.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■☐☐☐

Lebanon's offensive cyber capability is perceived to be mostly limited to surveillance or espionage operations, but there is no record of them making the jump to more disruptive or destructive tools.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
APT (Dark Caracal) (aka ATK 27, TAG-CT3) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Dark Caracal: Cyber-espionage at a Global Scale," Lookout and Electronic Frontier Foundation, January 18 2018. (2)	One APT group is believed to be affiliated with the Lebanese state. More specifically, it is believed to act under Lebanon's General Directorate of General Security (GDGS). It was first uncovered in 2007 and it has exfiltrated "hundreds of gigabytes" in at least 21 different countries, according to ThaiCERT (P.100). The stolen information usually includes company intellectual property and personally identifiable information. The group's targets are diverse, notably, military personnel, enterprises, medical professionals, activists, journalists, lawyers, and educational institutions. Level 1
"How Important Has Cyber Warfare Become to the States of the Middle East?," Kristina Kausch, February 1 2018.	According to the source, Lebanon is advancing from hiring hackers to actually using the software themselves. Level 2

Document	Excerpt
"EFF and Lookout Uncover New Malware Espionage Campaign Infecting Thousands Around the World," EFF, January 18 2018.	The article identifies one cyber operation sponsored by the Lebanese government: a 2018 espionage operation against some individuals of interest using malware infected apps: "People in the U.S., Canada, Germany, Lebanon, and France have been hit by *Dark Caracal*. Targets include military personnel, activists, journalists, and lawyers, and the types of stolen data range from call records and audio recordings to documents and photos." **Level 1**
"Volatile Cedar – Analysis of a Global Cyber Espionage Campaign," CheckPoint, March 31 2015. (1) "'Lebanese Cedar' APT," ClearSky, January 28 2021. (2)	The report describes the "Volatile Cedar" espionage campaign by the Lebanese Cedar APT. Check Point attributed this group to the Lebanese government or a political group in Lebanon. There are even indications that link the APT to the Hezbollah Cyber Unit. In 2021, a report by Clearsky uncovered new activity by the same APT against companies from the United States, the United Kingdom, Egypt, Jordan, Lebanon, Israel, and the Palestinian Authority, among others. The report reinstated the link between the APT and the Lebanese government. **Level 1**

Malaysia

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ■□□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber (2021)	Cyber Warfare Signals Regiment (99 RSPS) of the Malaysian Armed Forces
National Cyber Power Index (2020)	Ranked 24th when it comes to offense
National Cybersecurity Index (2022)	79.22 (19th)
Internet Penetration (2020)	90%
Internet Freedom Score	58/100 (Partly free)

Transparency Description

Malaysia's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. Malaysia has not officially declared to be in possession of offensive cyber capabilities. While underscoring the importance of developing cyber warfare capabilities and integrating them within military operations to counterbalance the regional opponents', such capabilities remain mostly aspirational and oriented towards the development of Cyber and Electromagnetic Activities (CEMA). From the outside, Malaysia's offensive capability is perceived to be currently limited to intelligence operations. However, sources highlight its aspiration to develop more sophisticated tools and capabilities.

Declared Capability Rating

Score ■□□□□

Malaysia increasingly underscores the importance of integrating cyber within military operations to counterbalance other Asia-Pacific countries, but overall, its declared capability remains aspirational for the time being and especially oriented towards the development of Cyber and Electromagnetic Activities (CEMA).

Data availability rating (1 being highest number of sources, 10 lowest): **7/10**

Document	Excerpt
"Defence White Paper 2020," Ministry of Defence, 2020.	"For the purpose of military operations, the combination of cyber operations with Electronic Warfare (EW) capabilities forms up the Cyber Electromagnetic Activities (CEMA) efforts to protect CNII." (pg. 27). It lists "Developing Cyber Electromagnetic Activities (CEMA) capability;" (pg. 46) as the second most important capability requirement for their 'future force'. "Hence, the MAF is planning to establish a Cyber Electromagnetic Command (CEC) to strengthen and coordinate CEMA. The responsibilities of the planned CEC will cover the following operations: i. Enhance Cyber Operations. Conduct cyber defence operations, cyber exploitation operation, cyberattack operation and develop cyber expertise, in line with the active defence concept as stipulated in MCSS; ii. Enhance Electronic Warfare (EW) Capabilities. Conduct electronic protection, EW support and electronic attacks; iii. Enhance Spectrum Management. Plan, coordinate and manage the use of the Electromagnetic Spectrum through operational procedures, engineering and administration to de-conflict all systems." (P. 53). **Level 1**

Document	Excerpt
"Malaysia Cyber Security Strategy 2020-2024," National Security Council Prime Minister's Department, October 12 2020.	"The development of a cyber-warfare capability is an important step towards counterbalancing the ability of other countries in the region and to defend important national targets from all forms of threats. It is important to stop any form of encroachment into national defence's computer systems and networks. Concurrently, it also provides the room for developing offensive capabilities for conducting cyber-operations when necessary. This capability would provide room for information fathering at strategic, operational and tactical levels."(P.13) Level 1
"Cyber warfare to be part of military 'future force'," FMT Reporters, November 4, 2019.	"Cyber warfare is to be a key component of the "future force" of the Malaysian Armed Forces, with a new command centre being set up to take charge of cyber defence operations. A highly-placed military official said the new Cyber Electromagnetic Command would oversee all cyber operations, taking over responsibility from the Malaysian Army. The official, who cannot be named, told FMT that cyber security is being taken seriously and will be a key component of the military's "future force". "The cyber command's main duties will be to neutralise external cyber threats, particularly those targeting strategic assets," the official told FMT." Level 1
"Malaysia's National Defence Policy", Ministry of Defence, July 2019	"The development of a cyber-warfare capability is an important step towards counterbalancing the ability of other countries in the region and to defend important national targets from all forms of threats. It is important to stop any form of encroachment into national defence's computer systems and networks. Concurrently, it also provides the room for developing offensive capabilities for conducting cyber- operations when necessary." (P. 13) Level 1

Perceived Capability Rating

Score ■■□□□

Malaysia's offensive capability is perceived to be mostly limited to intelligence operations, but is simultaneously considered to aspire for more sophisticated offensive capabilities to offset regional opponents.

Data availability rating (1 being highest number of sources, 21 lowest): **18/21**

Document	Excerpt
"Cyber Capabilities and National Power," IISS, 28 June 2021.	"Aside from the aspirations set out in the 2010 National Defence Policy and the 2020 defence white paper, there has been little indication of Malaysian activity in the sphere of offensive cyber." (P.157). In turn, Malaysian cyber aspirations are perceived to be set towards economic development rather than security. Level 1
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Malaysia is ranked number 24 in the cyber offense metric.
"Malaysia," UNDIR Cyber Policy Portal, April 2020.	About Malaysia's National Defence Policy the report indicates: "Concurrently, it also provides the room for developing offensive capabilities for conducting cyber-operations when necessary. This capability would provide the ability for information-gathering at strategic, operational and tactical levels." Level 2
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	"The National Defence Policy notes that cyber capabilities, both defensive and offensive, are necessary to 'counterbalance' other Asia–Pacific countries." (P. 51). Level 2

Mexico

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■☐☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	37.66 (84th)
Internet Penetration (2020)	72%
Internet Freedom Score	60/100 (Partly free)

Transparency Description

Mexico's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. Mexico has not officially declared to be in possession of offensive cyber capabilities and it appears to be mostly focused on enhancing defensive measures to contrast cybercrime. Other states perceive Mexico's capabilities as limited to the use of spyware to carry out intelligence operations. In 2017, one sources reported on two cyber espionage operations allegedly sponsored by the Mexican government and targeted against journalists and lawyers.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability. Mexico appears to be more focused on enhancing defensive measures and combatting cybercrime.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"Estrategia Nacional de Ciberseguridad," Gobierno de Mexico, 2017.	Establishes the creation of the Sub commission of Cybersecurity presided by the Secretary of State through the CNS (Federal Police/ Scientific Division) [Original: "la creación de la Subcomisión de Ciberseguridad, la cual está presidida por la Secretaría de Gobernación a través de la CNS (Policía Federal /División Científica).] The commissions objectives are to: approve and publicise the Strategy; Follow up and coordinate the implementation of the ENCS (Estrategia Nacional de Ciberseguridad) in collaboration with the different agencies and entities of the APF; Promote inter-institutional collaboration and cooperation schemes on cybersecurity; and Promote collaboration and cooperation with the different stakeholders: civil society, private sector, technical and academic communities [Original: Aprobar y dar a conocer la Estrategia; Dar seguimiento y coordinar la implementación de la ENCS en colaboración con las diferentes dependencias y entidades de la APF; Impulsar los esquemas de colaboración y cooperación interinstitucional en materia de ciberseguridad; y Fomentar la colaboración y cooperación con los diferentes actores interesados: sociedad civil, sector privado, comunidades técnicas y académicas.] It moreover, enumerates several defensive objectives like protecting critical infrastructure and building resilience. Level 0

Document	Excerpt
"Programa para la Seguridad Nacional 2014 – 2018," Consejo de Seguridad Nacional, April 30 2014. (1) "The State of Cybersecurity in Mexico: An Overview," Luisa Parraguez Kobe, January 2017. (2)	"The Programme focuses on specific policy for cybersecurity to protect and promote national interests and the main undertakings outlined within are to: promote actions to prevent and combat cyber-attacks; strengthen mechanisms for preventing incidents in the Federal executive sites; uphold compliance and development of procedures to evaluate and strengthen the performance of the response teams to incidents of cyber security in the Federal executive branch; improve human capital skills and technological infrastructure to address cyber security incidents; establish international cooperation on cyber security and cyber defense in particular with North American countries to prevent and address attacks on the computer systems of the country." ((2) P.10-11) **Level 0**

Perceived Capability Rating

Score ■□□□□

Mexico's offensive cyber capability is perceived to be limited to intelligence operations or spyware acquired from foreign vendors.

Data availability rating (1 being highest number of sources, 21 lowest): **20/21**

Document	Excerpt
"Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware," John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, June 19 2017.	The source identifies two cyberoperations sponsored by the Mexican government: both were espionage-based and targeted journalists. The software used was made by the Israeli company NSO Group and has been used by numerous other states. **Level 1**
"Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014.	Mexico has acquired surveillance and intelligence tools from the Italian private company Hacking Team. **Level 1**

Morocco

Cyber Transparency Score Untransparent

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	70.13 (30th)
Internet Penetration (2020)	84%
Internet Freedom Score	53/100 (Partly free)

Transparency Description

Morocco's scores for the declared and perceived capability rating differ considerably at the lower-end of the spectrum. Morocco has not officially declared to be in possession of offensive cyber capabilities. From the outside, Morocco is perceived as to use off-the-shelf spyware tools acquired from foreign vendors. In this regard, in 2019 Amnesty International reported on the alleged use by Morocco of NSO Group's Pegasus software to spy upon human rights activists.

Declared Capability Rating

Score

No official indication of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score

Morocco's offensive cyber capability appears to be mostly limited to off-the-shelf spyware acquired from commercial foreign vendors, but beyond that, there is no mention of more sophisticated and integrated offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 21 lowest): **18/21**

Document	Excerpt
"Morocco: Human Rights Defenders Targeted with NSO Group's Spyware," Amnesty International, October 10 2019.	Morocco was deemed in 2019 to be responsible for using the NSO Group's Pegasus software to spy upon some human rights activists. Level 1
"Kingdom of Morocco: Cyber Readiness at a Glance," Melissa Hathaway and Francesca Spidalieri, December 2018.	"Although Morocco has developed several cyber-related capabilities, there is no evidence that it has formalized the military or the intelligence services' cyber security mission in a policy or decree. The Royal Moroccan Armed Forces (FAR) is responsible for overseeing the development of cyber security and cyber defense capabilities and for ensuring the resilience and availability of the nation's military operational networks (i.e., air defense, air surveillance, ground surveillance, and special communications). It is also responsible for securing the networks and exchange of data among the three military components (i.e., army, navy, and air force)." (P. 24). Level 2
"How BAE sold cyber-surveillance tools to Arab states," BBC, June 14 2017.	Morocco was found to have bought cybersurveillance tools from a British/Danish company. Level 1
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	Morocco has acquired surveillance and intelligence tools from the Italian private company Hacking Team. Level 1

Netherlands

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber (2021) Defensie Cyber Commando

National Cyber Power Index (2020) Ranked 5th overall and 9th for cyber offensive capabilities

National Cybersecurity Index (2022)	83.12 (17th)
Internet Penetration (2020)	91%
Internet Freedom Score	n/a

Transparency Description

The Netherland's scores for the declared and perceived capability rating differ slightly at the middle-end of the spectrum. The Netherlands is transparent about its offensive cyber capability and future aspirations. The 2018 Cyber Strategy expressly underscores that an effective deterrence posture requires both the ability and credible capability to attack, and the latest Cyber Strategy (2021) signaled the intention by the Dutch government to develop offensive cyber assets and units. To fulfil such goals, the Netherlands recently established a Cyber Command that is mandated, *inter alia*, to carry out offensive cyber operations. Despite being vocal about the importance of offensive capabilities, limited details about the structure of the Cyber Command have been disclosed to date, and the Netherlands has yet to publish a military doctrine that concretely links the deployed means to the aims pursued. This notwithstanding, Dutch cyber capabilities are held in higher regard by foreign actors compared to domestic sources, often referring to prominent operations carried out by the Dutch Intelligence Agency which have been consistently reported on.

Declared Capability Rating

Score ■■■□□

The Dutch government has publicly disclosed it has offensive cyber capabilities in its Defence Cyber Strategy. Beyond that, it has published limited details on its cyber command structure, does not link concrete means and goals to this overall capability, and has yet to publish a detailed cyber defence doctrine. The government also confirmed that such an offensive capacity has not been used so far (until June 2017).

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"Countermeasures ransomware-attacks" Minister of Foreign Affairs, 6 October 2021	In a letter to parliament, the Minister of Foreign Affairs of the Netherlands describes that, under strict legal conditions, the Defence Cyber Command is allowed to use offensive cyber means against another state. Level 3
"Defence Cyber Strategy," Ministerie van Defensie, 2021.	"Developing offensive cyber assets and preparing guidelines for the preparation of cyber units and assets with a flexible design; developing cyber assets and cyber intelligence assets for tactical use." Level 3
"Defence Cyber Command," Ministerie van Defensie, last accessed in December, 2021.	"Defence Cyber Command concentrates on 3 areas of cyber security, one of which is defined as follows: Offensive capabilities: the armed forces sees offensive cyber capabilities as digital resources the purpose of which is to influence or pre-empt the actions of an opponent by infiltrating computers, computer networks and weapons and sensor systems so as to influence information and systems. The Netherlands Defence organisation deploys offensive digital resources exclusively against military targets." Level 3

Document	Excerpt
"Defensie Cyber Strategie 2018," Ministerie van Defensie, November 2018.	"A good defence and security are not enough to deter attackers from carrying out digital attacks. More and more allies are therefore taking a more active stance in the digital domain. In the context of both the first and the third main task, a more active contribution of defence within the existing structures is necessary [...] Deterrence makes the Netherlands a less attractive target for (cyber)attacks and is therefore a means of conflict prevention before everything. In addition to the ability to attack, deterrence requires credible offensive capabilities. By integrating into (ongoing) missions and operations, the Ministry of Defence will work to improve the visibility and credibility of its digital military capabilities." (P. 6-7) **Level 3**
Parliamentary Commission Foreign Affairs: questions about the International Cyber Strategy to the Minister of Foreign Affairs, Parliament of the Netherlands, 23 June 2017	In a response to questions from parliament, the Dutch Foreign Minister stated that to date [answered 23 June 2017] no offensive cyber capacity has been used. **Level 0**

Perceived Capability Rating

Score ■■□□□

The Dutch offensive cyber capability is domestically perceived to be lagging behind, mostly in terms of manpower, funds and mandate, while foreign sources rank the Dutch capability relatively high, which may be attributed to the visible cyber-enabled (counter-)intelligence capability of its intelligence services. While some perceive the Netherlands as to having integrated their offensive capability into their military structure, to date no offensive cyber operation has been disclosed or reported on which had disruptive or destructive effects.

Data availability rating (1 being highest number of sources, 21 lowest): **17/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	The Netherlands is placed 9th for cyber offense abilities.
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	The source lists the Netherlands' military cyber operations as in a state of growth in 2018 (P. 7). **Level 2**
"The Cyberarmy can and may not do much", NRC, 18 December 2018	This newspaper article expresses concerns about the limited mandate and capability of the Dutch Defence Cyber Command, emphasising the shortage of manpower and funds. The respective commander at the time expressed understanding of the criticism, explaining that it takes time to set up a new command. **Level 2**
"Dutch agencies provide crucial intel about Russia's interference in us elections," Volkskrant, 25 January 2018	Dutch newspaper de Volkskrant describes how the Dutch intelligence agency, AIVD, was able to infiltrate into the Russian Cozy Bear group, providing evidence that the group carried out cyber operations against the US DNC. Because this was an intelligence operation carried out by the civilian intelligence branch without disruptive or destructive effects, it remains labelled as level 1. **Level 1**
"The Netherlands Cyber Readiness at a Glance," Melissa Hathaway and Francesca Spidalieri, May 2017.	The report identifies that the Netherlands has been investing in and developing offensive cyber capabilities (P. 29). **Level 2**

New Zealand

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ■□□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	Ranked 15th overall and joint bottom for offensive
National Cybersecurity Index (2022)	51.95 (63rd)
Internet Penetration (2020)	92%
Internet Freedom Score	n/a

Transparency Description

New Zealand's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. New Zealand has not officially declared to be in possession of offensive cyber capabilities and it appears to be the Five Eyes member with the least developed cyber arsenal. While having underscored the need to provide the military with relevant combat capabilities to conduct cyber operations in the 2018 Strategic Defence Policy Statement, to date the development of offensive capabilities remains mostly aspirational. Accordingly, outside sources perceive New Zealand as to focus on defensive capabilities. No past operations have been directly attributed to New Zealand.

Declared Capability Rating

Score ■□□□□

The New Zealand government has alluded to the need to develop offensive cyber capabilities, but unlike most of its Five Eyes counterparts, it has not publicly acknowledged to be in possession of such a capability.

Data availability rating (1 being highest number of sources, 10 lowest): **9/10**

Document	Excerpt
"Cyber Security and Support Capability," Website New Zealand Ministry of Defence, Last Accessed February 18 2022.	"The Cyber Security and Support Capability (CSSC) will develop an enhanced Defensive Cyberspace Operations (DCO) capability (people, processes, policies and technologies) that protects, defends and contributes to the resilience of NZDF networks, systems and platforms including deployed force elements." Objectives include: "(1) To uplift the NZDF's military cyber capability to protect and defend networks, platforms and systems, (2) Address DCO capability build required; such as skillsets (3) Provide coherence and become the centralised unit that delivers the cyber capability uplift; and (4) Work collaboratively with the BAU cyber functions to ensure current activities are aligned with the future uplift" Level 0
"Strategic Defense Policy Statement," New Zealand Government, July 2018.	"To maintain relevant combat capabilities, including interoperability with close partners, into the future the Defence Force needs to be able to conduct a broader range of cyber operations. This would provide military commanders with a broader set of tools to achieve military objectives and respond to activities that threaten both New Zealand security and the safety of Defense Force personnel." Level 1

Perceived Capability Rating

Score 

New Zealand is perceived to lag behind its Five Eyes allies when it comes to offensive cyber capabilities, although it is considered to show interest in developing said capability. The only public reference found to an offensive operation was not directly attributed to New Zealand but more generally to the Five Eyes community.

Data availability rating (1 being highest number of sources, 21 lowest): **18/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	NZ is ranked as the 15th most comprehensive cyber power and joint bottom for offensive cyber abilities (alongside 13 other states).
"Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts – sources," Christopher Bing, Jack Stubbs, Joseph Menn, June 27 2019.	The report identifies New Zealand as one of the potential state sponsors (as part of the Five Eyes) behind the 2019 compromise of Yandex. Given that this operation is not specifically attributed to one nation, it remains a level 0. **Level 0**
"Predicting the Proliferation of Cyber Weapons into Small States," Daniel Hughes and Andrew Colarik, October 1 2016.	According to this paper, New Zealand's cyber policy is mainly defensive: "In key New Zealand defense documents, references to cyber primarily mention defense against cyber-attacks, with only two references to the application of military force to cyberspace. There is no mention of cyber weapon acquisition." (P. 22). Nonetheless, the paper claims that New Zealand "most likely has the technical capability to adapt existing cyber weapons or develop new ones, particularly if aided by its allies" but that "Due to fiscal constraints, however, any additional funding for cyber weapons will likely have to come from the existing defense budget and thus result in compromises to other capabilities." (P. 22). This report actually determines that "New Zealand is unlikely to gain significant benefits from the acquisition of cyber weapons. This is due to its limited military capabilities, multilateral foreign approach, extensive participation in international organizations, and pacifistic security identity." (P. 25). **Level 0**
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	This report describes there being some ambiguity on the extent of New Zealand's cyberpower: some sources define it as simply improving the traditional armed forces, other sources claim that New Zealand is developing a cyber capability as a new significant weapon. **Level 2**

Nigeria

Cyber Transparency Score Transparent and Low Capability

Declared Capability Rating ■■□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber	Army Cyber Warfare Command
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	54.55 (56th)
Internet Penetration (2020)	36%
Internet Freedom Score	59/100 (Partly free)

Transparency Description

Nigeria's scores for the declared and perceived capability rating are identical at the lower-end of the spectrum. In 2016, the Army reported to the press on the establishment of a Cyber Warfare Command explicitly focused on "cyberwarfare". The unit is tasked with monitoring, defending, and assaulting in cyberspace through distributed DDoS attacks against terrorists, insurgent criminal groups, as well as hostile nation states. However, to date, no further details, strategies, or doctrines detailing offensive cyber operations have been disclosed. Nigeria's cyber capabilities are perceived as still limited to surveillance and intelligence tools which it acquires from foreign vendors, and some observers tend to be sceptical about Nigeria's in-house capacity.

Declared Capability Rating

Score ■■□□□

Nigeria has established an Army Cyber Warfare Command, which is charged with offensive cyber operations. No further details, strategies or doctrines were found detailing its offensive cyber programme.

Data availability rating (1 being highest number of sources, 10 lowest): **9/10**

Document	Excerpt
"Modern Battle Not Limited to Land, Air and Maritime Domain – COAS," Nigerian Army, October 9 2021.	The Chief of Army Staff (COAS), Lieutenant General Faruk Yahaya identified cyberspace as another domain of war and noted that "there is need for requisite manpower to effectively operate in that space." "This – he further said – is necessary to build capacity that will enhance the proficiency of personnel to counter these threats. He noted that, to this end, NACWS among other roles, was established to provide specialist training for cyber warriors, aimed at inducting trained cybersecurity specialists to the NACWC and other cyber affiliated formations in support of Nigerian Army operations." In regard to capacity building, he adds: "the nation's security dynamics imply that efforts must be re-doubled with needed cyber products and competencies to defeat all forms of cyber threats confronting the nation." Level 0
"Nigerian Army's Cyber Warfare Command begins operation," Vanguard, August 29 2018	The report states that "Military sources told Vanguard that the highly technical Command would be initially composed of 150 ICT specially trained officers and men drawn from all the Corps and Services in the Nigerian Army" and that the Cyber Warfare Command "is charged with the responsibility to monitor, defend and attack subversive elements in the cyberspace." In regards to the capacity to do so, the military sources added that the Command had the "capacity to protect the Nations Critical Infrastructure" and that "Plans have been concluded to send officers and soldiers of the command to attend various courses in Countries like US, Russia and the UK." Level 2

Perceived Capability Rating

Score ■■□□□

In 2016, Nigeria became the first African nation to set up a cyber command centre, with an explicit focus on "cyberwarfare", therefore appearing to aspire to offensive cyber capabilities. Some observers who have noticed these developments are sceptical of the in-house capacity, as its current capability remains mostly limited to surveillance and intelligence tools acquired from foreign vendors. No publicly available attacks or operations have been attributed to Nigeria.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"The Nigerian Cyber Warfare Command: Waging War In Cyberspace," Kate O'Flaherty, November 26 2018.	Numerous news reports detail the creation of a Nigerian Cyber Warfare Command in 2016. This is comprised of 150 trained officers. However, some outside observers are sceptical of the expertise of this unit. Most people believe that the vast majority of this unit will simply be formed by re-trained soldiers with little to no background in cybersecurity. Others have commented: "I think it is posturing," Vanderburg says. "They have resisted some of the cooperation from the US – we had the US-Africa Command, for example." Level 2
"The Nigerian Cyber Warfare Command: Waging War In Cyberspace," Kate O'Flaherty, November 26, 2018.	"In 2016, the Nigerian Army announced plans to take the war against insurgency to the nation's cyberspace. The result is the Nigerian Army's Cyber Warfare Command: According to reports, 150 IT trained officers and men drawn from the corps and services in the Nigerian Army. Their aim: to monitor, defend and assault in cyberspace through distributed denial of service (DDoS) attacks on criminals, nation states and terrorists." Level 2
"Here Are All the Sketchy Government Agencies Buying Hacking Team's Spy Tech," Janus Rose, July 6 2015.	In one instance, Nigeria was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. Level 1

Norway

Cyber Transparency Score Transparent and High Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■■□□

Organization for Offensive Cyber	The Norwegian Armed Forces
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	62.34 (45th)
Internet Penetration (2020)	97%
Internet Freedom Score	n/a

Transparency Description

Norway's scores for the declared and perceived capability rating are identical in the middle of the spectrum. Norway has declared to be in possession of offensive cyber capabilities. In 2018, the Department of Defence officially acknowledged that Norwegian intelligence services are tasked with planning and conducting offensive operations, including cyberattacks (Computer Network Attacks), and the Minister of Defence confirmed that Norwegian armed forces do possess offensive cyber capabilities. However, no details, strategies, operational plans, or military doctrines have been disclosed so far. Compared to other European counterparts, Norway is much less vocal about its capabilities. One report noted that, despite possessing a branch of the armed forces called Cyber Defence, the latter is not strictly a cyber command since it only directs defensive cyber operations.

Declared Capability Rating

Score ■■■□□

Norway has been transparent about obtaining offensive cyber capabilities, but no further details are disclosed by means of a publicly-available and dedicated military strategy or doctrine.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"Forsvarsministeren bekrefter: Norge har offensive cyber-våpen," ALF Bjarne Johnsen, June 27, 2019.	"The Norwegian Armed Forces have access to offensive cyber capabilities. The conflict between the US and Iran shows how offensive cyber weapons are now being deployed in military operations." Level 3
"Bakke-Jensen: Norge har offensive cyberapasiteter," Christian Bugge Hjorth, June 27, 2019.	"To VG's question whether Norway has offensive cyber capabilities, the Minister of Defence answers as follows: The Armed Forces has offensive capabilities. Then there will be an assessment via FOH (the Armed Forces' operational headquarters) how they can possibly be used. It is the E-service that has the offensive capabilities. Then it is the Cyber Defence that has the defensive. And then you are subject to FOH, corresponding to army, air and sea, he says." Level 3

Document	Excerpt
"Høringsnotat: Forslag til ny lov om Etterretningstjenesten," Forsvarsdepartementet, November 12, 2018.	"The intelligence service has the national responsibility for planning and conducting offensive cyber operations, including cyber attacks (Computer Network Attack), as well as coordinating between offensive and defensive cyber measures in the Armed Forces. The intelligence service is also responsible for providing intelligence attribution of foreign threat actors in serious cyber operations aimed at Norway or Norwegian interests. Legally, these tasks fall outside the framework of a law concerning the collection and processing of information, and the legality of the actions must therefore be assessed specifically based on the circumstances." [Original: Etterretningstjenesten har det nasjonale ansvaret for å planlegge og gjennomføre offensive cyberoperasjoner, herunder cyberangrep (Computer Network Attack), samt koordinere mellom offensive og defensive cybertiltak i Forsvaret. Etterretningstjenesten har også ansvaret for å forestå etterretningsmessig attribusjon av utenlandske trusselaktører ved alvorlige cyberoperasjoner rettet mot Norge eller norske interesser. Rettslig sett faller disse oppgavene utenfor rammen av en lov som dreier seg om innhenting og behandling av informasjon, og legaliteten av handlingene må derfor vurderes konkret ut fra omstendighetene.] (P. 113) **Level 3**
"Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren," Forsvarsdepartementet, March 1 2014.	"CNE and CNA are considered offensive activities and is normally carried out in an opponent's network. CNE shall help to search for, capture, identify and locate activities and information in the cyber domain of the purpose of achieving situational awareness and in order to recognize threats" (P.6) [Original: CNE og CNA er å anse som offensive aktiviteter og gjennomføres normalt i en motstanders nettverk. CNE skal bidra til å søke etter, fange opp, identifisere og lokalisere aktiviteter og informasjon i cyberdomenet i den hensikt å oppnå situasjonsforståelse og for å kunne gjenkjenne trusler.] "The armed forces shall have the capacity for offensive cyber operations, which among other things contributes to protect us from attacks from the outside. Like any other use of military means, these the capacities subject to political control and strategic management, cf. also mention of CNA and CNE section 3.7.1." (P.13) [Original: Forsvaret skal ha kapasitet for offensive cyberoperasjoner, som bl.a. bidrar til at vi kan beskytte oss mot angrep utenfra. Som all annen bruk av militære maktmidler er også disse kapasitetene underlagt politisk kontroll og strategisk styring, jf. også omtale av CNA og CNE i punkt 3.7.1. Ytterligere regulering av offensive cyberoperasjoner er gradert og fastsatt i annet regelverk og dokumentasjon.] **Level 1**
"Prop. 73 S (2011-2012) A Defense of Our Time," Norwegian Government, 2011-2012.	"The digital space is already an important battle arena, and it is important that the further modernization of the Armed Forces take into account to be able to carry out both defensive and offensive operations in this field." [Original: Det digitale rom er allerede en viktig stridsarena, og det er viktig at den videre moderniseringen av Forsvaret tar høyde for å kunne gjennomføre både defensive og offensive operasjoner på dette feltet.] **Level 1**

Perceived Capability Rating

Score 

Norway's offensive cyber capability is perceived to be more restrained than those of its European counterparts. It is perceived to be less overt or vocal about this capability, in part perhaps because it still mainly resides within the intelligence community.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"Norway's secret surveillance of Russian politics at the NSA," Dagbladet, 2020.	"The head of the NIS [Norwegian Intelligence Service] has stated that they are using all available assets in keeping an eye on the High North. The mission of the intelligence service is not restricted to purely military objects of interest, but is to work within all areas of interest to Norwegian government." Level 2
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The authors note, when comparing Dutch and Norwegian offensive cyber capabilities, that "the Norwegians are much more restrained and focused on counter-intelligence than the 'vocal' Dutch with their offensive means. Norway also possesses a cyber command (P. 187) that deals only with defensive cyber operations. However, "Compared to these countries, Norway lags behind in the development of doctrine, and education and training." (P. 193). This is reinforced by the fact that Norway's cyber command's budget "was a modest €197,000," (P. 194) while Denmark, on the other hand, spends 9 million euros year on theirs. Level 2
"Preparing for Cyber Conflict Case Studies of Cyber Command," Piret Pernik, December 2018.	The article notes that Norway possesses offensive cyber-space capabilities, and makes the claim that this has been publicly confirmed (P. 1), but also notes that the capability primarily resides within the intelligence community: "Even though Norway has a branch of the armed forces called Cyber Defence, it does not constitute a cyber command in the above narrower sense because it directs and controls only defensive cyberspace operations, while offensive and ISR operations are directed and controlled by the Norwegian Intelligence Service subordinated to CHoD." (P. 4). Level 3

Pakistan

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	42.86 (77th)
Internet Penetration (2020)	25%
Internet Freedom Score	25/100 (Not free)

Transparency Description

A lack of transparency is observed for Pakistan. Pakistan has not officially declared to be in possession of offensive cyber capabilities. However, Pakistan is perceived as to having some forms of offensive capabilities, although mostly limited to intelligence and defacement operations through state-sponsored hacking groups against its neighbouring rivals. Indeed, several APTs have been attributed to Pakistan or are suspected to be sponsored by the government.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■■☐☐

Pakistan is perceived to have offensive cyber capabilities, mostly deployed against its neighboring rival during periods of geopolitical tension, although their extent is largely unknown. Beyond that, it is mostly linked to several state-sponsored hacking groups that carry out intelligence operations and defacements.

Data availability rating (1 being highest number of sources, 21 lowest): **14/21**

Document	Excerpt
APT (Aggah)"Aggah Using Compromised Websites to Target Businesses Across Asia, Including Taiwan Manufacturing Industry," Anomali August 12 2021.	This group was first noted in 2019 and is believed to be sponsored by Pakistan. It bears similarities to the Gorgon Group, a Pakistani group "known for targeting Western governments" and its TTPs contain Urdu language. Its attacks usually focused on the UAE are now targeting the Far East. In July 2021, the APT was found to be conducting a spear-phishing campaign against manufacturing firms in Taiwan and South Korea. Level 3
APT (Gorgon Group) (aka Subaat, ATK 92, TAG-CR5) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	This APT is active since at least 2017 and it is suspected to have links to Pakistan, but a government link has yet to be formally confirmed. Its attacks have been directed towards government organizations in the United Kingdom, Spain, Russia, and the United States. In 2017, the group executed a small spear-phishing campaign against US-based government organization. In 2018, the group were targeting organisations the United Kingdom, Spain, Russia, and the United States. Moreover, they were also carrying out criminal activity in tandem. Level 0

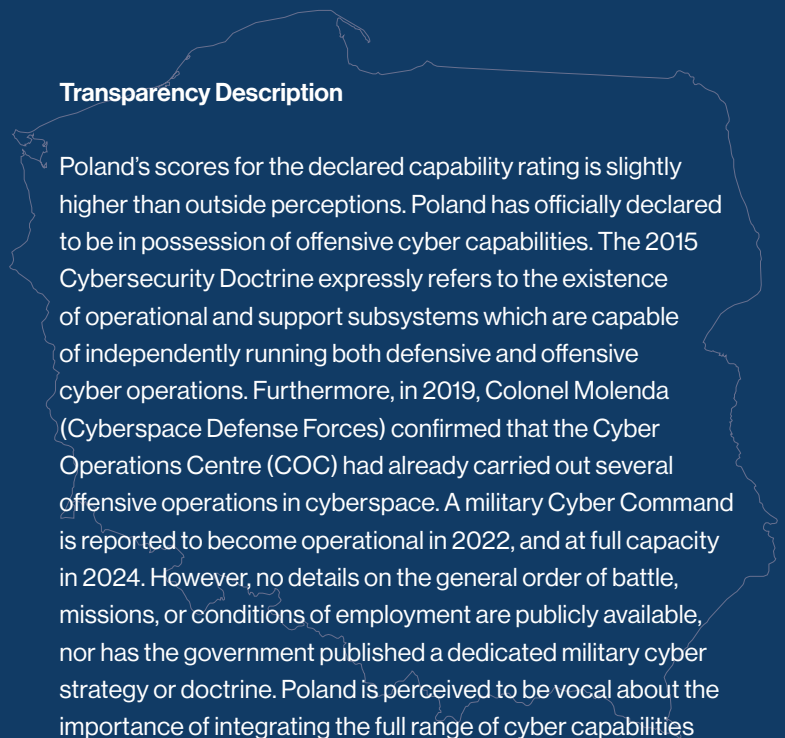
Document	Excerpt
APT36 (aka Mythic Leopard, Transparent Tribe, TMP.Lapis, ProjectM, C-Major) "APT36 jumps on the coronavirus bandwagon, delivers Crimson RAT," Malwarebytes Labs, March 16 2020. (1) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (2)	Active since at least 2016, APT 36 is likely sponsored by Pakistan. In 2016, a spear phishing operation dubbed "Transparent Tribe" was uncovered against officials at Indian embassies in both Saudi Arabia and Kazakhstan. In the same year, the group was found to be "collecting data about Indian troop movements using an Android app called SmeshApp."((2) P.345). The actors also carried out Operation "C-Major," a spear phishing campaign targeted Indian military officials and infecting their devices through an Adobe vulnerability. Most recently, in 2020, the group launched a spear-phishing campaign through a fake Indian government health advisory. **Level 1**
APT (Stealth Mango and Tangelo) "Stealth Mango & Tangelo Selling your fruits to nation state actors," Lookout, 2018	This APT executes "highly targeted intelligence gathering campaign" and is believed to be "operated by members of the Pakistani military." The report notes that "this actor has used ... surveillanceware tools to successfully compromise the mobile devices of government officials, members of the military, medical professionals, and civilians." And goes on to state: "To date, we have observed Stealth Mango being deployed against victims in Pakistan, Afghanistan, India, Iraq, Iran, and the United Arab Emirates. The surveillanceware also retrieved sensitive data from individuals and groups in the United States, Australia, and the United Kingdom". Because the targets align with Pakistani interests, it is possible that the group is state-sponsored. **Level 1**
"Information Warfare: Emerging Arena for Future Conflicts," Premjit Singh Panesar, 2017.	The author, a former Indian military official, claims that Pakistan has had cyberwarfare capabilities since 1998, when it began defacing Indian websites (P. 54). He also suspects Pakistan has funded several hacker groups (P. 54). **Level 2.5**
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	The source notes that Pakistan is "said to possess both defensive and offensive cyber capabilities, although their extent is largely unknown. Most often deployed against neighbouring India during periods of increased geopolitical tension, this capacity is most probably housed within the Directorate General for Inter-Services Intelligence." (P. 63). **Level 3**
"Achieving cyberdeterrence and the Ability of Small States to Hold Large States at risk ," Jason Rivera, 2015.	Rivera (2015) suggests that Pakistan has a government-sponsored cyberwarfare programme (P. 21). **Level 2**

Poland

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■□□□



Transparency Description

Poland's scores for the declared capability rating is slightly higher than outside perceptions. Poland has officially declared to be in possession of offensive cyber capabilities. The 2015 Cybersecurity Doctrine expressly refers to the existence of operational and support subsystems which are capable of independently running both defensive and offensive cyber operations. Furthermore, in 2019, Colonel Molenda (Cyberspace Defense Forces) confirmed that the Cyber Operations Centre (COC) had already carried out several offensive operations in cyberspace. A military Cyber Command is reported to become operational in 2022, and at full capacity in 2024. However, no details on the general order of battle, missions, or conditions of employment are publicly available, nor has the government published a dedicated military cyber strategy or doctrine. Poland is perceived to be vocal about the importance of integrating the full range of cyber capabilities within its overall military structure, and sources reported that the government's commitment to create a cyber command dates back to 2008. To date, no offensive cyber operations has been attributed to Poland.

Organization for Offensive Cyber (2022)	Cyberspace Defence Forces (Wojska Obrony Cyberprzestrzeni)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	87.01 (9th)
Internet Penetration (2020)	83%
Internet Freedom Score	n/a

Declared Capability Rating

Score ■■■□□

Poland had disclosed that it can carry out offensive cyber operations. Its military Cyber Command is reported to be operational in 2022, and at full capacity by 2024. No further details on its general order of battle, missions, conditions of employment or are publicly available, nor has it published a dedicated military cyber strategy or doctrine.

Data availability rating (1 being highest number of sources, 10 lowest): **9/10**

Document	Excerpt
"Wojsko ma "doświadczenie w prowadzeniu operacji ofensywnych" w cyberprzestrzeni," Andrzej Kozlowski, February 28, 2019.	"The panel concluded that the COC [cyber command] was already operating across the full operational spectrum, does this mean that offensive operations in cyberspace have already been carried out? The Cyber Operations Centre already has some experience in cyberspace operations. I personally participated in several of them together with COC soldiers. I can tell you about one, during which I had the pleasure of leading three teams of specialists of the center, as part of the Anaconda-16 exercises. It was probably the first time in NATO's history that cyber operations were conducted in real-world ICT systems for the exercise. Such actions required the approval of the Minister of National Defence and contributed significantly to raising awareness of the dangers among senior military executives. The exercise was that COC specialists interacted with our networks to play a scenario of enemy penetrating." Level 3
"Cybersecurity doctrine of the Republic of Poland 2015," Poland, 2015.	"Operational and support subsystems - capable of independently running defensive (protective and defense) and offensive cyber operations, as well as providing and receiving support as part of allied operations." (P. 9) Level 3

Perceived Capability Rating

Score 

Poland is perceived to be vocal on the importance of integrating the full range of cyber capabilities within its overall military structure, although more details on its implementation has not been concretely documented. No cyber operations have been attributed to Poland. In one instance, Poland was found to have acquired surveillance and intelligence tools from a foreign vendor.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The book notes that Poland has been committed to creating a cyber command since 2008, but the progress of that commitment is commented upon. (P. 187). **Level 2**
"Poland Unveils Cyber Defence Plans," Warfare Today, September 13 2019.	The article observes that Poland is committed to having a 2000-soldier strong cyber unit. It should be operational by 2022, and at full capacity by 2024. **Level 2**
"Polish prime minister urges allies to beef up Cybersecurity budgets," Ashish Kumar Sen, January 16 2019.	The article notes that the Polish PM said during a recent conference: "I call on you today and encourage your leaders and governments *to spend more money on cyber warfare, as we do,* on cyber soldiers to protect our Internet frontier." Moreover, the PM also sought deeper cooperation with the U.S. on cyber issues. **Level 2**
"National Cyber Security Organisation: Poland," Joanna Świątkowska, Izabela Albrycht, Dominik Skokowski, 2017.	The document analyses Polish defence documents that state Polish security should be achieved "by developing both defensive and offensive capabilities." (P. 9). Other documents have also noted this idea: "[The National Security Strategy of the Republic of Poland] stipulates the need for development of both defensive and offensive cyber capabilities along with new units within the Armed Forces dedicated to this goal. The National Security Strategy also stresses the need to enhance preparedness for any incidence of cyber war and the country's ability to react, either unilaterally or with the cooperation of allies." (P. 15). "...there is an imperative to develop defensive and offensive cyber Capabilities." (P. 15). **Level 2**
"Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014.	In one instance, Poland was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
" Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	CSIS claims that "Poland will create an "Independent Information Force" in the armed forces to integrate electronic intelligence, psychological operations, and cyberoffensive and defensive actions." (P. 40). **Level 2**

Qatar

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	58.44 (49th)
Internet Penetration (2020)	100%
Internet Freedom Score	n/a

Transparency Description

Qatar's scores for the declared and perceived capability rating differ considerably at the lower-end of the spectrum. Qatar has not officially declared to be in possession of offensive cyber capabilities. Yet it is perceived as having some type of offensive capability, although mostly limited to spyware tools used in cyber-enabled espionage operations. In this regard, a prominent cyberespionage operation carried out by Qatar against 1400 individuals in several countries has been reported on in 2019. Concurrently, other sources detail that Qatar is planning to acquire more advanced offensive capabilities to target regional adversaries.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Document	Excerpt
"Qatar National Cyber Security Strategy 2014," Ministry of Information and Communications Technology, May 2014.	The document lists 5 key objectives, the fifth of which being: "Objective 5: Develop and cultivate national cyber security capabilities." (P. 9). However, later elaboration seems to suggest that these capabilities are primarily defensive in nature: "Development of a national cyber security research and development agenda that is focused on building solutions to prevent, predict, and overcome cyber attacks will further prepare Qatar for emerging cyber threats. Existing data analytics and social computing capabilities will enable Qatar to pursue an agenda that supports the application of real-time data analytics to detect cyber attacks, conduct forensics and remediate cyber events, and anticipate and ultimately defeat cyber attacks." (P. 12) Level 0

Perceived Capability Rating

Score 

Qatar's offensive cyber capability is perceived to be mostly limited to spyware acquired from foreign vendors and cyber-enabled espionage operations. It was reported that the government also reached out to US firms to acquire more advanced offensive capabilities, potentially to target regional adversaries.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
" The State of Qatar's Hack of Democracies: A Global Cyber-crime Operation," Richard Miniter, March 30 2019.	The document identifies Qatar as having conducted a cyber-espionage operation against 1400 individuals living abroad, including U.S. and UN officials and ambassadors. **Level 1**
"How BAE sold cyber-surveillance tools to Arab states," BBC, June 14 2017.	The article claims that Qatar was found to have bought cyber-surveillance tools from a British/Danish company. **Level 1**
"As cyberwarfare heats up, allies turn to U.S. companies for expertise," Ellen Nakashima, November 22 2012.	The article details how Qatar was planning to acquire offensive capabilities from an American firm. This is especially motivated by the cyber capabilities of hostile neighbors including Saudi Arabia and Iran. It explains that "In the spring of 2010, a sheik in the government of Qatar began talks with the U.S. consulting company Booz Allen Hamilton about developing a plan to build a cyber-operations center". This supposedly included offensive capabilities, triggering a negative response from the US company. **Level 2**

Russia

Cyber Transparency Score Very Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■■■

Organization for Offensive Cyber	Intelligence agencies
National Cyber Power Index (2020)	Ranked 4th with a score of 28.38 and 3rd when it comes to offence
National Cybersecurity Index (2022)	71.43 (28th)
Internet Penetration (2020)	85%
Internet Freedom Score	30/100 (Not free)

Transparency Description

A complete lack of transparency is observed for Russia. Russia has never officially disclosed to be in possession of offensive cyber capabilities, nor details regarding order of battle, types of effects, TTPs, or military doctrines have ever been published. However, Russia is widely recognised as a cyber power with a highly capable offensive cyber arsenal established within its intelligence services. Recorded offensive operations attributed to or considered to be affiliated with the Russian government are countless and have been widely documented following the numerous intelligence reports, public attributions, sanctions, and indictments carried out by other states. They cover a wide range of cyber operations, from espionage, attacks against critical infrastructure, and information warfare to cyber and electromagnetic activities (CEMA). While some APTs are directly linked to intelligence agencies, other APTs are only loosely affiliated with the government, offering a degree of plausible deniability. The listed operations are by no means exhaustive, and they all indicate a highly advanced capability as well as a strong resolve to deploy them.

Declared Capability Rating

Score ☐☐☐☐☐

No official disclosure of offensive capability was found by the Russian government. Its National Security Strategy (originally published in 2009) is supplemented by more recent publications covering 'information security' that reflect Russia's conception of cyber as a component of information warfare and psychological operations. Most notably, its doctrine of information security distinguishes between two forms of informational attacks: the technical and psychological. The doctrine is mostly concerned with the latter, and nearly all technical attacks (including cyber and electronic attacks) are coordinated or supplemented with a psychological effect in mind. However, no offensive capability is publicly disclosed by the government.

Data availability rating (1 being highest number of sources, 10 lowest): **9/10**

Document	Excerpt
"Doctrine of Information Security of the Russian Federation," Russian Federation, December 5, 2016.	The doctrine distinguishes between two forms of informational attacks: the technical and psychological. It is mostly concerned with the latter, and nearly all technical attacks (including cyber and electronic attacks) are coordinated or supplemented with a psychological effect in mind. The doctrine does not disclose details on Russian offensive cyber capabilities. Level 0
"Russia's National Security Strategy to 2020," Russian Federation, May 12, 2009.	"Strategic deterrence presupposes the development and systemic realisation of a range of interconnected political, diplomatic, military, economic, informational and other measures, intended to forestall or reduce the threat of destructive action on the part of a state aggressor (coalition of states)." (P. 4) Level 0

Perceived Capability Rating

Score ■■■■■

Russia is perceived of having a highly capable offensive cyber capability driven by its intelligence services. It has one of the longest track records in offensive activity that covers a wide range of cyber operations, from espionage, attacks against critical infrastructure, information warfare, to cyber and electromagnetic activities (CEMA), which have been well documented following the numerous public attributions, sanctions, indictments, and intelligence reports. Moscow has demonstrated a willingness to employ offensive cyber in situations other than war to affect political and economic outcomes in neighbouring nations and to deter its adversaries. The government's passive support or direction – rather than tight restriction and direction – of non-state hackers and criminals has been widely reported on. While some APTs are directly linked to intelligence agencies, other APTs are only loosely affiliated with the government, offering a degree of plausible deniability. The listed operations are by no means an exhaustive list, but indicative of its highly advanced capability.

Data availability rating (1 being highest number of sources, 21 lowest): **2/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Russia is ranked as the fourth overall cyber power and ranked third for offensive cyber power. **Level 5**
"Cyber Operations Tracker," Council on Foreign Relations, 2020.	According to the tracker, 86 offensive cyber operations were attributed to Russia. Some of these attributed operations include: numerous attacks on a variety of government institutions and think tanks, the 2017 NotPetya attack, attacks on electricity grids and critical infrastructure in Ukraine, attempted election interference in the US in 2016, and the 2007 DDoS attack on Estonia. This is but a small selection of the more significant events. These operations have been a mixture of different types of cyber power. **Level 5**
APT 29 (aka Cozy Bear, The Dukes, Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, Cloudlook, Grizzly Steppe, ATK7, Cozer, Cozy Car, Euro APT, Hammer Toss, Office Monkeys, Sea Duke, TDISCOVER, UPLOADER) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign," November 19 2018. (2)	APT29 is a cyberespionage group attributed to the Russian Foreign Intelligence Service (SVR). The group's targets include Western governments and organizations. At a smaller scale, the group also attacks Asian, African and Middle Eastern governments. In June 2016, this group was involved in the Democratic National Committee breach. Most recently, in 2019, the group has carried out a phishing campaign multiple industries in the US (military, imagery, transportation, pharmaceutical, national government, and defense contracting.) **Level 5**
APT (Turla) (aka Turla Group, Waterbug, Venomous Bear, Group 88, SIG23, Iron Hunter, Pacifier APT, Hippo Team, Krypton, PFINET, Popeye, Snake, TAG_0530, Uroburos, Wraith, ATK13, MAKERSMARK, CTG-8875, ITG12) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The Turla Group is attributed to FSB. It is known for having carried out information theft and espionage campaigns in 45 different countries. Targets range from government, embassies, military, education, research to pharmaceutical companies. Its first recorded operation was in 1996. Most recently, the group targeted in January 2020 two Ministries of Foreign Affairs in Eastern Europe and one national parliament in the Caucasus region. **Level 5**
APT (TeleBots) (aka Sandworm Team) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Russian Military Intelligence: Background and Issues for Congress," CRS, November 15 2021. (2) "New WannaCryptor-like ransomware attack hits globally: All you need to know," ESET, June 27 2017. (3)	The group, attributed to GRU Unit 74455 (2), has targeted high-profile targets within the Ukranian sector. It bears similarities with other groups like Sandworm Team, Iron Viking and Voodoo Bear. The group is allegedly responsible for the NotPetya ransomware/ supply-chain attacks. The group executed cyberattacks against various computer systems in Ukraine; compromising critical infrastructure and other businesses in the nation. **Level 5**

Document	Excerpt
APT (Temp.Veles) (aka Xenotime, MAR-17-352-01 HATMAN, Triton, Trisis, Triton Group, ATK91) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "TRISIS: Analyzing Safety System Targeting Malware," Robert M. Lee, December 14 2017 (2) "Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure," Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, Christopher Glyer, December 14 2017 (3) "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas," Dragos, June 14 2019 (4)	The group has been attributed to Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM). It specializes in sabotaging and destroying critical infrastructure. The group uses TRITON, a malware action that can compromise industrial safety systems. There are three recorded attacks by Temp.Veles. One in 2014 using TRISIS malware against safety instrumented systems (SIS) in the Middle East causing operational disruption (2), another one in 2017 against a critical infrastructure organization attempting to "manipulate industrial safety systems" with TRITON malware (3) and a similar one in February 2019 (4). **Level 5**
APT 28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackeral, Iron Twilight, Grizzly Steppe, ATK5, Group-4127, TAG_0700, Iron Twilight) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group has been attributed to GRU Unit 26165 and Unit 74455. In 2016, APT 28 allegedly interfered in the US elections by undermining Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee. At present, APT 28 is said to collect intelligence on Eastern European governments. This information is of interest to Russia since it could give the Russian government the upper hand in influencing public opinion in these countries. **Level 5**
APT (Gamaredon Group) (aka Winterflounder, Primitive Bear) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group is attributed to FSB 16th and 18th centers. It specializes in information theft and espionage. The group is the author of the ongoing cyber espionage campaign "Operation Armageddon" which commenced in 2013 as a result of developments in the Ukraine-Europe Association Agreement. Throughout 2019, the group targeted Ukranian diplomatic, government and military officials. Last recorded attacks are in March and April 2020, using Covid19 content as a bait in phishing campaigns. **Level 5**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	Russia is known for having carried out offensive operations against various countries: "In addition to the now normal information disruption campaigns, Russia has been using cyberattacks on energy plants routinely for the past several years in the Russo-Ukrainian war with carefully timed and programmed outages." (P. 42). "In October 2018, Australia joined 21 international partners to call out Russia for a pattern of malicious cyber activity targeting political institutions, businesses, media, and sport. In October 2018, the Foreign Minister also condemned Russian cyber operations against the Organisation for the Prohibition of Chemical Weapons (OPCW) and flight MH17 investigation." (P. 282). **Level 5**
"The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5," Ryan C. Maness, June 1 2019.	The data identifies numerous cyberattacks they attribute to Russia. Key victims include the USA, Canada, the UK, France, Germany, Poland, Estonia, Lithuania, Ukraine, Georgia, and Turkey. **Level 5**
"Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom," Rod Thornton and Marina Miron, July 10 2019.	The article points out that "In Russian thinking, cyber warfare, as a subset of information warfare, is divided into two operational spheres: cyber-technical and cyber-psychological" (P. 259). Most of Russia's high-profile cyber operations "are designed to have psychological effect. These focus on either influencing electoral outcomes or on 'hack-and-leak' activity." (P. 261). Yet, less high profile operations consist of "covert intelligence-gathering operations and those aimed at putting in place malware 'to sit invisibly within networks enabling [the Russians] to launch a cyberattack should the order be given.'" (P. 261). **Level 4**
"Worldwide Threat Assessment of the US Intelligence Community," Daniel R. Coats, January 29 2019.	In the assessment, the US acknowledges Russia as a " a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve its political and military objectives. Moscow is now staging cyberattack assets to allow it to disrupt or damage US civilian and military infrastructure during a crisis and poses a significant cyber influence threat," (P. 5). In addition, the analysis notes that Russian cyberattacks have the ability to "generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016." (P. 6). **Level 5**

Document	Excerpt
"A New Kind of Information Warfare? Cyber-Conflict and the Gulf Crisis 2010-2017 ," Tarek Cherkaoui, August 2018.	"It is worth noting here that the Russian authorities also rely on a private contractor, namely the Internet Research Agency, to coordinate some of the Kremlin's digital influence operations. This measure offers the safety of plausible deniability if needed." (P. 16). **Level 4**
"Understanding Russian 'Hybrid Warfare' and what can be done about it," Christopher Chivvis, March 22 2017.	"The Kremlin now has access to a growing cadre of cyber warriors that allows it to hack into Western information systems to collect valuable information. The information is then used to influence elections and other political outcomes outside Russia's borders. This was the strategy Russia appears to have attempted during the 2016 U.S. presidential campaign. Beyond stealing secrets, Russia could deploy more advanced cyber tools to directly manipulate or otherwise affect the information systems on which Western political processes rely. There is no evidence that Russia possesses such capabilities today, but if Western defenses are not strengthened, it may develop them." (P. 3). **Level 4**
"Russia's Approach to Cyber Warfare," Michael Connell and Sarah Vogler, September 2016.	The paper claims that the Georgian conflict, while successful, brough to light a number of organizational deficiencies. As a result, "the Ministry of Defense (MOD) announced—along with other military reforms—that it would establish a branch in the military responsible for conducting information operations, complete with specially trained and equipped troops." (P. 6). Nowadays, "Cyber hacking groups, or advanced persistent threat (APT) groups, have become a central part of Russia's cyber IO toolkit. While direct links to the Russian government are difficult to prove conclusively (and the Russian government denies that it sponsors any hacker groups), there are a number of groups whose activities closely align with Kremlin and Russian military objectives." (P. 7). **Level 5**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	The report states that "The Military Doctrine of 2010 discusses the use of political and informational instruments to protect national interests and those of allies. The Doctrine defines the characteristic features of modern military conflict as including the integrated use of military force and non-military capabilities, and a greater role for information warfare." **Level 4**
Suspected affiliation to the Russian Federation	
"SSU identifies FSB hackers responsible for over 5,000 cyber attacks against Ukraine (video)," SSU, November 4 2021.	Ukraine attribution of 2021 cyberattacks to Russia: "The SSU Cyber Security Department identified hackers of the notorious ARMAGEDON group, which carried out over 5,000 cyberattacks against public authorities and critical infrastructure of Ukraine. They are officers of the 'Crimean' FSB and traitors who defected to the enemy during the occupation of the peninsula in 2014". **Level 5**
"Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes," Council of the EU, September 24 2021.	EU attribution of 2021 Ghostwriter cyber incidents: "Some EU Member States have observed malicious cyber activities, collectively designated as Ghostwriter, and associated these with the Russian state. Such activities are unacceptable as they seek to threaten our integrity and security, democratic values and principles and the core functioning of our democracies." **Level 5**
"Ukraine says Russian hackers hit its Navy website," Reuters, July 9, 2021.	Ukrainian attribution of 2021 cyberattack against its navy: "Ukraine's defence ministry said that hackers linked to the Russian authorities on Friday attacked the website of the Ukrainian Naval Forces and published fake reports about the international Sea Breeze-2021 military drills." **Level 4**
"FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," The White House, April 15 2021 (1) "Russia: UK exposes Russian involvement in SolarWinds cyber compromise," UK Government, April 15 2021 (2) "Declaration by the High Representative on behalf of the European Union on respect for the EU's democratic processes," Council of the EU, September 24 2021 (3)	US attribution of 2020 SolarWinds cyberattack: "Today the United States is formally naming the Russian Foreign Intelligence Service (SVR), also known as APT 29, Cozy Bear, and The Dukes, as the perpetrator of the broad-scope cyber espionage campaign that exploited the SolarWinds Orion platform and other information technology infrastructures. The U.S. Intelligence Community has high confidence in its assessment of attribution to the SVR." The UK (2) government and the EU (3) backed the US attribution of SolarWinds to Russia **Level 5**

Document	Excerpt
"Sanctions by the Numbers: Spotlight on Cyber Sanctions," Jason Bartlett and Megan Ophel, May 4 2021.	Since 2012, the US Treasury Department has issued more than 140 cyber-related sanctions against Russian individuals and entities, oftentimes linked to branches of the Russian government. **Level 5**
"FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," The White House, April 15 2021.	Following the 2020 SolarWinds attack, the Biden Administration sanctioned 6 Russian technology companies having provided support to the Russian intelligence cyber programme. Biden also sanctioned 32 entities and individuals for their attempt to influence the 2020 US elections **Level 5**
"Issuance of Executive Order Blocking Property With Respect To Specified Harmful Foreign Activities Of The Government Of The Russian Federation and related Frequently Asked Questions; Russia-related Designations," US Department of Treasury, April 15 2021.	In 2021, 35 additional Russian individuals and entities were sanctioned for their role in malicious cyberattacks. **Level 5**
"Swedish sports body hacked by Russians, officials say," AP News, April 13 2021.	Swedish attribution of 2017 Swedish Sport Confederation hack: "The organization that oversees Sweden's national sports federations was hacked by Russian military intelligence in 2017-18, officials said Tuesday, in a data-breaching campaign that also affected some of the world's leading sporting bodies, including FIFA and the World Anti-Doping Agency." **Level 5**
"France identifies Russia-linked hackers in large cyberattack," Laurens Cerulus , February 15 2021. (1) "Rapport Menaces et Incidents du CERT-FR," CERT-FR, February 15 2021. (2)	France attribution of 2017-2020 cyberattack to Russia: "The agency said it had identified "an intrusion campaign" in which hackers, linked to Russian military intelligence agency GRU, compromised the French software firm Centreon in order to install two pieces of malware into its clients' networks" (2) **Level 4**
"Consolidated List of Financial Sanctions Targets in the UK," Office of Financial Sanction Administration HM Treasury, December 31 2020.	After Brexit, The UK implemented the sanctions against the same individuals and entities targeted by the EU. **Level 5**
"Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Official Journal of the European Union, October 22 2020.	Two GRU agents were sanctioned by the EU for their role in the 2015 German Bundestag attack. One entity, the 85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), was sanctioned for its role in the 2015 German Bundestag attack **Level 5**
"UK and partners condemn GRU cyber attacks against Olympic and Paralympic Games," NCSC October 19 2020.	UK attribution of 2020 Olympic and Paralympic Games attempted cyberattacks: "The UK has today (19th October) exposed malicious cyber activity from Russia's GRU military intelligence service against organisations involved in the 2020 Olympic and Paralympic Games before they were postponed. (...)The National Cyber Security Centre (NCSC), a part of GCHQ, assesses with high confidence that these attacks were carried out by the GRU's Main Centre for Specialist Technologies (GTsST), also known as Sandworm and VoodooBear." **Level 5**
"UK and partners condemn GRU cyber attacks against Olympic and Paralympic Games," NCSC, October 19 2020.	UK attribution of 2018 Olympic Games cyberattacks to Russia: According to the NCSC, "In the attacks on the 2018 Games, the GRU's cyber unit attempted to disguise itself as North Korean and Chinese hackers when it targeted the opening ceremony. It went on to target broadcasters, a ski resort, Olympic officials and sponsors of the games." **Level 5**
"Six Russian GRU Officers Charged with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace: Unsealed Indictment," US District Court Western District of Pennsylvania, October 19 2020.	US attribution of 2017 Macron presidential campaign hack to Russia: the US Department of Justice indicted six Russian nationals for their role, among other cyberattacks, in "spear-phishing campaigns in and around April and May 2017 targeting local government entities, political parties, and campaigns, including now French President Emmanuel Macron's "La Republique En Marche!" political party in connection with Macron's 2017 presidential campaign"(P.3) **Level 5**

Document	Excerpt
"Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," US Department of Justice, October 19 2020.	In 2020, the US Department of Justice indicted six GRU officers, within Unit 74455, for their role in worldwide deployment of malware and other cyber operations aimed at supporting the Russian governments. The press release specifically identifies their targets as: Ukraine (BlackEnergy, KillDisk, etc), Georgia (spearphishing, network compromise and website defacement), French elections (spear phishing and hack-and-leak), NotPetya, efforts to ensure Russian accountability for Novichok use (spearphishing), and the 2018 PyeongChang Winter Olympic Games (Olympic Destroyer) **Level 5**
"Norway blames Russia for cyber-attack on parliament," BBC News, October 13 2020	Norway attribution of 2021 Parliament cyberattack: "Foreign Minister Ine Eriksen Soreide called it a serious incident affecting the country's "most important democratic institution." "Based on the information available to the government it is our assessment that Russia stood behind this activity" she said without giving any evidence." **Level 4**
"Report of the Select Committee on intelligence United States Senate on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election. Volume 5: Counterintelligence Threats and Vulnerabilities," U.S. Senate, August 18 2020.	US attribution of 2016 DNC hack and interference in presidential elections to Russia: according to the Senate Intelligence Committee report on the Russian role in the 2016 presidential elections, "The Committee found that the Russian government engaged in an aggressive, multifaceted effort to influence, or attempt to influence, the outcome of the 2016 presidential election." **Level 5**
"COUNCIL IMPLEMENTING REGULATION (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Official Journal of the European Union, July 30 2020.	Four GRU agents were sanctioned for their role in the attempted cyber operation against the OPCW. **Level 4**
"COUNCIL IMPLEMENTING REGULATION (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States," Official Journal of the European Union, July 30 2020.	One entity, the Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), was sanctioned for its role in the NotPetya attack. **Level 5**
"Advisory: APT29 targets COVID-19 vaccine development," NSCS, July 16 2020.	UK, US ad Canadian attribution of 2020 attempted COVID-19 vaccine cyber attack to Russia: "The United Kingdom's National Cyber Security Centre (NCSC) and Canada's Communications Security Establishment (CSE) assess that APT29 (also known as 'the Dukes' or 'Cozy Bear') is a cyber espionage group, almost certainly part of the Russian intelligence services. The United States' National Security Agency (NSA) agrees with this attribution and the details provided in this report. (...) Throughout 2020, APT29 has targeted various organisations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines." **Level 5**
APT (Sandworm Team) (aka Iron Viking, Voodoo Bear, Quedaegh, TEMP.Noble, Black Energy, Electrum, Telebots, ATK14, Hades/OlympicDestroyer, CTG-7263) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group is linked to Unit 74455 of the GRU, and has mainly targeted Ukrainian infrastructure, government, and media sectors. For instance, in December 2015, the group provoked widespread power outages in Ukraine. The group was also found to be behind NotPetya. **Level 5**
APT (Inception Framework)(aka Inception Group, ATK116, Cloud Atlas, the Rocra, Oxygen, Red October) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Operation red October: the astonishing hacking ring that shook the world," Adaware, September 17 2021. (2) "Recent Cloud Atlas activity," Securelist, August 12 2019. (3)	The group is with a sophisticated toolkit to attack high-profile targets such as executives in the oil, finance or engineering sectors and government, diplomatic and military officials. The group first started targeting individuals inside of Russia or directly related to Russian interest but the group has now extended its attacks to targets abroad. Attacks include: Operation "RedOctober" a long term espionage campaign, stealing sensitive information such as diplomatic secrets to personal information from multiple leading infrastructural entities in different countries (2) and Operation "Cloud Atlas," a series of spear phishing attacks against targets in Russia, Central Asia and regions of Ukraine with ongoing military conflicts (3). The group was not explicitly linked to a specific government entity, but was considered to be state-sponsored. **Level n/a**

Document	Excerpt
APT (Energetic Bear) (aka Dragonfly, Crouching Yeti, Group 24, Koala Team, Iron Liberty, Electrum, ATK 6, Havex, TG-4192, Dymalloy) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "Ukraine's power outage was a cyber attack: Ukrenergo," Pavel Polityuk, Oleg Vukmanovic, Stephen Jewkes, January 18 2017. (2) "New Insights into Energetic Bear's Watering Hole Cyber Attacks on Turkish Critical Infrastructure," Yonathan Klijnsma, November 2 2017 (3). "'State-sponsored' hackers targeted EirGrid electricity network in 'devious attack'," Cathal McMahon, August 7 2017. (4)	The group is specialized in cyberespionage operations on the energy sector. It has been active since at least 2011 and has carried out attacks in 38 different countries. The groups Dragonfly and Dragonfly 2.0 bear similarities but are tracked separately. The most recent attacks were on the energy sector of Ukraine in 2016, resulting in a power outage. In 2017 the group launched an attack on "a website belonging to a Turkish energy company ... being used in a watering hole attack targeting people associated with Turkish critical infrastructure (3). Finally, on the same year the group compromised the routers used by EirGrid, the company that controls the power grids in the country, in Wales and Northern Ireland (4). This group was not explicitly linked to a specific government entity, but was considered to be state-sponsored. **Level n/a**
APT (Berserk Bear) (aka Dragonfly 2.0, Dymalloy) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," CISA, March 15 2018 (2) "Russian state hackers behind San Francisco airport hack," Catalin Cimpanu, April 14 2020 (3)	Drangonfly 2.0 has been active since at least 2016, having attacked US critical infrastructure and government entities with sabotage and destruction attacks. In May 2017, the group attacked energy companies critical infrastructure both in Europe and the US (2). In March 2020 the group attacked the San Francisco airport (3). This group was not explicitly linked to a specific government entity but is thought to be state-sponsored by Russia. **Level n/a**
"Merkel blames Russia for 'outrageous' cyberattack on German parliament," Hans von der Burchard , May 13 2020.	Germany attribution of 2015 Bundestag cyberattack to Russia: "Angela Merkel said she had "hard evidence" that Russia was responsible for an "outrageous" cyberattack on the German parliament. The German chancellor said the hacking attack, which occurred in 2015 and also targeted her own parliamentary email account, "obviously disturbs a trustful cooperation" with Russia." **Level 5**
"Georgia is targeted by Russia in a disruptive cyber-attack,"The Embassy of Georgia to the USA, March 2, 2020.	Georgian attribution of 2019 cyberattacks to Russia: "The Ministry of Foreign Affairs of Georgia announced that investigations had proved that the Russian General Staff Main Intelligence Directorate (GRU) Main Center for Special Technologies had carried out a "widespread, disruptive cyber-attack" against web pages and servers of Georgian government agencies, courts, and media organizations on October 28, 2019." **Level 4**
"Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses Resulting in Tens of Millions in Losses and Second Russian National Charged with Involvement in Deployment of "Bugat" Malware," US Department of Justice, December 5 2019	In 2019, the US Department of Justice indicted two Russian nationals: Maksim Yakubets, on charges of international computer hacking and bank fraud schemes, and Igor Turashev for his role in the Bugat malware. The investigation was pursued in partnership with the UK National Crime Agency. No specific link to the government is mentioned. **Level n/a**
"Czech Republic blames Russia for multiple government network hacks," Catalin Cimpanu, December 3 2018.	Czech attribution of 2018 MFA cyber attack to Russia: according to ZDNet, "The Czech Security Intelligence Service (BIS) blamed two cyber-espionage groups --known as Turla and APT28 (Sofacy or Fancy Bear)-- for hacks of the Ministry of Foreign Affairs (MFA), Ministry of Defense, and the Army of the Czech Republic. The hacks took place in different campaigns across 2016 and 2017." **Level 4**

Document	Excerpt
"Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW," Ministerie van Defensie, October 4 2018. (1) "Joint statement by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and High Representative / Vice-President Federica Mogherini," European Commission, October 4 2018 (2) "Statement by NATO Secretary General Jens Stoltenberg on Russian cyber attacks," NATO, October 4 2018. (3) "Reckless campaign of cyber attacks by Russian military intelligence service exposed," NCSC, October 2018. (4)	Dutch attribution of attempted 2018 OPWC cyberattack to Russia: "On 13 April 2018, with support from the Netherlands General Intelligence and Security Service and UK counterparts, the Netherlands Defence Intelligence and Security Service (DISS) disrupted a cyber operation being carried out by a Russian military intelligence (GRU) team. The Russian operation had targeted the Organisation for the Prohibition of Chemical Weapons (OPCW) in The Hague" (1). The attribution was supported by the EU (2), NATO (3), and the UK (4). **Level 4**
"U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," US Department of Justice, October 4 2018.	In 2018, the US Department of Justice indicted seven officers of the Russian Main Intelligence Directorate (GRU) for several crimes, including computer hacking. According to the DOJ press release, the computer intrusions followed the beginning of the investigation into Russian state-sponsored doping at the 2014 Sochi Winter Olympics. **Level 5**
"Reckless campaign of cyber attacks by Russian military intelligence service exposed,"NCSC, October 3 2018. (1) "UK and Australia blame Russian GRU for quartet of cyber attacks," Chris Duckett, October 4 2018. (2)	UK attribution of series of cyberattacks to Russia: the "NCSC assess with high confidence that the GRU was almost certainly responsible" for the 2017 BadRabbit Ransomware; the 2016 hack-and-leak of the World Anti-Doping agency; the 2016 DNC hack; and the 2015 cyberattack against a small UK-based TV station. Australia supports these attributions. **Level 5**
"Deputy Attorney General Rod J. Rosenstein Delivers Remarks Announcing the Indictment of Twelve Russian Intelligence Officers for Conspiring to Interfere in the 2016 Presidential Election Through Computer Hacking and Related Offenses," US Department of Justice, July 13 2018.	In 2018, the US Department of Justice indicted "twelve Russian military officers for conspiring to interfere with the 2016 presidential elections". The defendants allegedly work for two units within the GRU, and were tasked with stealing and leaking information **Level 5**
"Treasury Sanctions Russian Federal Security Service Enablers," US Department of the Treasury, June 11 2018.	In 2018, two Russian entities were sanction by the Trump Administration for providing material and technological support to the FSB. **Level 5**
"Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," US Department of Justice, February 15 2018.	In 2018, the US Department of Justice charged thirteen Russian citizens and three Russian entities for seeking to interfere with the US political system and the 2016 elections. According to the press release, the defendants engaged in information warfare to spread mistrust towards the political system. The conspiracy was part of operation "Project Lakhta". No direct government control is mentioned, but these are considered to be at least sanctioned by the government. **Level n/a**
US "Russian Military was Behind the NotPetya attack, CIA concludes," Ellen Nakashima, January 12 2018. (1) UK "US joins UK in blaming Russia for NotPetya cyber-attack," Sarah Marsh, February 15 2018.Denmark, Lithuania, Estonia, Canada and Australia. (2) "Blaming Russia for NotPetya was coordinated diplomatic action," Stilgherrian, April 12 2018. (3)	Several nations have attributed the 2017 NotPetya cyberattacks to Russia: in the US "The CIA has attributed to Russian military hackers a cyberattack that crippled computers in Ukraine last year, an effort to disrupt that nation's financial system amid its ongoing war with separatists loyal to the Kremlin". In the UK "British defence secretary, Gavin Williamson, accused the Russian government of "undermining democracy" with the attack, which primarily targeted Ukraine's financial, energy and government sectors before ." Five other nations attributed the NotPetya attacks to Russia: Denmark, Lithuania, Estonia, Canada and Australia. Statement of supports were issued by New Zealand, Norway, Latvia, Sweden and Finland **Level 5**
"Russia hacked Danish defense for two years, minister tells newspaper,"Reuters, April 23 2017.	Danish attribution of 2017 Danish Defense Ministry hack to Russia: according to Reuters, the official Danish Defense Intelligence Service report did not mention the country behind the attack, however "Foreign Minister Claus Hjort Frederiksen told Berlingske it was Russia." **Level 5**

Document	Excerpt
"IAAF says medical records compromised by Fancy Bear hacking group," Brian Homewood, April 3 2017.	IAAF attribution of 2017 IAAF hack to Russia: according to a Reuters article, "The IAAF said in a statement the hacking group known as Fancy Bear, which has been linked by western governments and security experts to a Russian spy agency blamed for some of the cyber operations that marred the 2016 U.S. election, was believed to be behind the attack of medical records in February." **Level 5**
"U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," US Department of Justice, March 15 2017.	In 2017, the US Department of Justice indicted four Russian citizens for their role in the 2014 Yahoo hack. Of these four defendants, two were identified as officers of the Russian Federal Security Service (FSB) **Level 5**
"GRIZZLY STEPPE – Russian Malicious Cyber Activity," NCCIC and FBI, December 29 2016.	US attribution of Agent.btz malware having caused the 2008 cyberattacks to Russian military and civilian Intelligence Services: "This Joint Analysis Report (JAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This document provides technical details regarding the tools and infrastructure used by the Russian civilian and military intelligence Services (RIS) to compromise and exploit networks and endpoints associated with the U.S. election, as well as a range of U.S. Government, political, and private sector entities"(P.1) **Level n/a**
"FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment," The White House, December 29 2016.	Following the Russian interference in the 2016 US elections, the Obama Administration sanctioned nine Russian entities and individuals: the Gru, the FSB, four GRU officers, and three entities having provided support to GRU's operations **Level 5**
"WADA Confirms Attack by Russian Cyber Espionage Group," WADA, September 13 2016	WADA attribution of 2016 WADA cyberattack to Russia: according to its press release, "The World Anti-Doping Agency (WADA) confirms that a Russian cyber espionage group operator by the name of Tsar Team (APT28), also known as Fancy Bear, illegally gained access to WADA's Anti-Doping Administration and Management System (ADAMS) database via an International Olympic Committee (IOC)-created account for the Rio 2016 Games." **Level 5**
"U.S. official blames Russia for power grid attack in Ukraine," Evan Perez, February 12 2016.	US attribution of 2015 Ukrainian power outage to Russia: according to a CNN article Elizabeth Sherwood-Randall, former deputy Energy Secretary under the Obama Administration, said that Russia was behind the cyberattack against the Ukrainian power grid. **Level 5**
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	In one instance, Russia was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
"Remarks by Secretary Carter at the Drell Lecture Cemex Auditorium, Stanford Graduate School of Business, Stanford, California," Defense Secretary Ash Carter, April 23 2015.	US attribution of 2015 Pentagon Legacy System hack to Russia: in a speech Secretary Carter said "Earlier this year, the sensors that guard DoD's unclassified networks detected Russian hackers accessing one of our networks. (...) After learning valuable information about their tactics, we analyzed their network activity, associated it with Russia, and then quickly kicked them off the network, in a way that minimized their chances of returning." **Level n/a**
"SSU repels information psychological attack of Russian special service," SSU, 12 September 2014.	Ukraine attribution of 2014 attempted email compromise to Russia: in a press release, the Security Service of Ukraine stated that it had "detected and disrupted another information subversion of the Russian special services aimed at obtaining illegal access to the personal data of the Ukrainian citizens and governmental internal information. (...) It has been established that the attacks were directed from a single control center of the Russian special forces". **Level 4**

Saudi Arabia

Cyber Transparency Score Untransparent

Declared Capability Rating ■□□□□

Perceived Capability Rating ■■■□□

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020) Ranked 26th overall and joint last when it comes to offence	
National Cybersecurity Index (2022)	83.12 (14th)
Internet Penetration (2020)	98%
Internet Freedom Score	24/100 (Not free)

Transparency Description

A lack of transparency is observed for Saudi Arabia. The government has not officially declared to be in possession of offensive cyber capabilities, and a purely aspirational objective to develop such capabilities has been included in an official report drafted by the government in the occasion of former U.S. President Trump's visit to Saudi Arabia in 2017. However, Saudi Arabia is perceived as to having acquired spyware tools from foreign vendors and as having engaged in espionage operations against foreign journalists and dissidents by using NSO Group's Pegasus malware. It has also been reported that Saudi Arabia is willing to undertake hacking and surveillance operations against regional adversaries, such as Qatar, and that it is increasingly interested in developing more sophisticated cyber and electromagnetic capabilities.

Declared Capability Rating

Score ■□□□□

Almost no public information about the declared cyber capabilities of Saudi Arabia was found, except for aspirational statements.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Document	Excerpt
"Saudi Arabia and the Visit of Donald Trump: June 2017 Report," Saudi Arabia, June 2017.	In this Saudi-authored report, they put in the following update, one of the few times they even mention cyber capabilities: "RIYADH, Saudi Arabia, May 20, 2017 — In a ceremony witnessed by the Custodian of the Two Holy Mosques, King Salman bin Abdulaziz Al Saud, and U.S. President Donald J. Trump, Raytheon Company (NYSE: RTN) and the Saudi Arabia Military Industries Company today signed a Memorandum of Understanding to cooperate on defense-related projects and technology development. (...) This partnership will also contribute directly to the Kingdom of Saudi Arabia's localized defense ecosystem with regional expert capabilities, and will provide a long-term foundation for Saudi Arabia's economic development. "This strategic partnership is the next step in our over 50-year relationship in the Kingdom of Saudi Arabia and a strong indicator of our continued global growth," said Thomas A. Kennedy, Raytheon Chairman and CEO. "By working together, we can help build world-class defense and cyber capabilities in the Kingdom of Saudi Arabia." (P. 69) Level 1

Perceived Capability Rating

Score 

Saudi Arabia's offensive cyber capability appears to be mostly limited to spyware acquired from foreign vendors and intelligence operations. Recent reports, however, indicate a growing interest to develop more sophisticated cyber and electromagnetic capabilities.

Data availability rating (1 being highest number of sources, 21 lowest): **15/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	The index ranks Saudi Arabia's offensive cyber capabilities as joint last (alongside 13 other states), and 26th overall.
"Saudi Arabia Outsources Cyber Arsenal, Buys Spyware, Experts Say," Alyza Sebenius, January 28 2020. (2)	Many reports suggest Saudi cyber capabilities have been purchased from foreign private IT companies. While these "purchased weapons can be "highly sophisticated," they are "of limited scope," This means that "While Saudi Arabia has tools that can be technically complex, countries that have invested in developing indigenous offensive and defensive capabilities — such as Saudi Arabia's Middle Eastern neighbors Iran and Israel — possess a greater range of cyber weapons and tactics." Level 1
"The Rise of the Rest: Maturing Cyber Threats Beyond the Big Four," Zach Dorfman and Breanne Deppisch, November 2019.	"Although all three countries are U.S. security partners, Saudi Arabia and the UAE have acutely antagonistic relations with Qatar, and operations from both sides have targeted the other state or states." [...] The willingness of these states to undertake aggressive international hacking and surveillance campaigns could—and arguably has—helped further destabilize the Middle East." Level 3
"The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil," Bill Marczak, John Scott-Railton, Adam Senft, Bahr Abdul Razzak, and Ron Deibert, October 1 2018. (1)	The article attributes four cyber operations to the Saudi government, these are primarily espionage-based operations directed at foreign journalist and Saudi dissidents using NSO Group's Pegasus malware. Level 1
"Cybersecurity in the Middle East and North Africa," Valentina von Finckenstein, May 2018.	"Saudi Arabia suffers from the highest number of cyberattacks in the Middle East. The target is often Saudi critical infrastructure, in particular the energy sector." (P. 5). This has prompted significant Saudi investment in cyber capabilities, often supported by their close ally, the US. Level 2
"The Kingdom of Saudi Arabia Cyber Readiness at a Glance," Melissa Hathaway, Francesca Spidalieri, and Fahad Alsowailm, September 2017.	The article reports that "The only type of cyber security exercise reported occurred during the 2014 Saudi military exercises dubbed "Sword of Abdullah," which included training on electronic warfare," (P. 13). And that "...the Saudi National Guard is investing nearly half a billion dollars to develop an electronic warfare capability" (P. 22). Level 2
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	Saudi Arabia has acquired surveillance and intelligence tools from the Italian private company Hacking Team. Level 1

Singapore

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ■□□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber	Defence Cyber Command
National Cyber Power Index (2020)	Ranked 18th overall and joint last when it comes to offence
National Cybersecurity Index (2022)	71.43 (29th)
Internet Penetration (2020)	92%
Internet Freedom Score	54/100 (Partly free)

Transparency Description

Singapore's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. Singapore has not officially declared to be in possession of offensive cyber capabilities. Based on the few official documents available, it appears that Singapore's cyber capabilities are primarily cast within a defensive mold. Indeed, an Integrated Cyber Command has recently been established but its mandate is to undertake defensive operations to defend against foreign threats. Given its highly digitalized nature and its leading role in cyber, one could expect Singapore to have at least acquired offensive cyber capabilities. Yet, no cyber operation has ever been attributed to Singapore, and its current capabilities are perceived to be under development.

Declared Capability Rating

Score ■□□□□

Singapore's cyber capabilities are primarily cast within a defensive mold. While it has a Defence Cyber Command, no further details are disclosed on its offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
Ministry of Defence, Committee of Supply Debate 2020, Speech Minister for Defence Dr Ng Eng Hen, March 2 2020	The Minister of Defence announced that an integrated SAF Cyber Command is to be developed. It is primarily cast within a defensive mold, and no further details are available that explain how this concept is materialized in reality. Level 0
"POINTER Monograph No. 13," Ministry of Defence, 2019.	"States need a clear strategy of whether they seek deterrence by punishment, whether they can signal the desired behavior, and whether they can face consequences in the event of escalation." Level 0
"Singapore's Cybersecurity Strategy," Cyber Security Agency of Singapore, 2016.	"There is a need to implement more robust laws that allow for a more proactive approach to national cybersecurity." Level 1

Perceived Capability Rating

Score ■■□□□

Given its highly digitalised nature and its leading role in cyber diplomacy, Singapore is perceived to have at least acquired offensive cyber capabilities in theory. Yet, no operation has been attributed to Singapore and no other demonstrations of this hypothesized capability was perceived, beyond the impression that it is under development.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Singapore is ranked as the 18th most comprehensive cyber power. Its offensive cyber capabilities are ranked as joint last (alongside 13 other states).
"What's Behind Singapore's New Integrated Military Cyber Command Objective?," Prashanth Parameswaran, March 10, 2020.	"Of particular note were efforts to create an integrated cyber command to detect potential cyberattacks and defend Singapore. Per a statement placed on the Singapore defense ministry (MINDEF) website, a high-level committee, led by the Permanent Secretary (Defense Development) and Chief of Defense Force (CDF), "will guide restricting efforts to create an integrated Cyber Command to defend our digital borders, especially against foreign cyber actors." Few additional specifics were provided regarding this integrated SAF Cyber Command. But the statement noted that the SAF Cyber Command "will provide threat assessments and early warning of cyberattacks, and respond accordingly," and that the new restructuring would better enable MINDEF and SAF to achieve its mission." No direct reference to offensive capabilities is made. **Level 0**
"A Small State Perspective on the Evolving Nature of Cyber Conflict: Lessons from Singapore," Eugene E.G. Tan, January 2020.	The article prefaces the discussion on cyber power by stating that many states do not want to fully reveal the extent of their cyber capabilities for various reasons. It then quotes a Singaporean minister: "there are only a few countries in the world who have shown this level of sophistication when it comes to cyberattacks.(. .) We are not able to reveal more because of operational security reasons." (P. 165). The paper also states: "Singapore has not used its cyber capabilities offensively." (P. 165). **Level 0**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The book lists Singapore as one state "considered possessing substantial military cyberspace capabilities and some of these countries have announced intentions to create cyber commands and/or cyberattack capabilities," (P. 188). **Level 2**
"Singapore Ramps Up Its Cyber War," Prashanth Parameswaran, March 8 2017.	Parameswaran (2017) argues that in response to prominent cyberattacks, Singapore has been increasing the number and training of cyber defenders, and also setting up a new cyber command (which would be comprised of 4 formations and 2600 soldiers). **Level 0**
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	"Singapore's military capabilities in cyberspace are reported to be among the best developed in Asia. It has publicly stated its interest in developing both offensive and defensive cyber capabilities as far back as its 2000 Defence White Paper. The Defence Technology Group, the Defence Sciences and Technology Agency and the Defence Science Organisation all contribute to Singapore's military technical developments. The Singapore Armed Forces also maintain the Cyber Defence Operations Hub, which protects Singapore's military networks, and it was recently announced that the number of personnel assigned to the hub would double by 2020. Despite Singapore's deep technical capabilities, the military's strategic discussions on the use of cyberspace appear to be underdeveloped." (P. 71). **Level 2**

South Africa

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ■□□□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber	Cyberwarfare Command Centre Head Quarter (unconfirmed)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	36.36 (88th)
Internet Penetration (2020)	70%
Internet Freedom Score	73/100 (Free)

Transparency Description

South Africa's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. To date, South Africa has not officially declared to be in possession of offensive cyber capabilities. In 2015 and 2017, South Africa announced that it was willing to establish a Cyberwarfare Command Centre Head Quarter and a Cyber Warfare Strategy, which supposedly included a reference to the development of offensive capabilities. However, such statements have remained aspirational as no further details regarding the structure, core principles, and mandate of the cyber unit have been released. South Africa is perceived as developing offensive cyber capabilities, albeit lacking significant progress.

Declared Capability Rating

Score ■□□□□

South Africa claimed it would establish a Cyberwarfare Command Centre HQ and a Cyber Warfare Strategy in which a reference was made to offensive information warfare actions. Since that announcement, no further details were found on the progress of the Command Centre, the strategy or further details on its offensive capability.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"Department of Defence Annual Report 2019/2020," Ministry of Defence, March 31 2020.	"According to the DoD 2019/2020 Annual Report, the Cyber Warfare Strategy has not yet been submitted to the Justice, Crime Prevention and Security Cluster (JCPS)" Level 0
"Department of Defence Annual Performance Plan for 2017," Department of Defence, March 16, 2017.	"During the FY2016/17 the DoD has developed a comprehensive departmental Cyber Warfare Strategy aligned with the national policy regarding South Africa's posture and capabilities related to offensive information warfare actions." (P. 6-7) Level 1
"National Cybersecurity Policy Framework (NCPF)," State Security Agency, December 4 2015.	In order to protect its interests in the event of a cyber-war, a cyber defence capacity has to be built. The NCPF thus promotes that a Cyber Defence Strategy, that is informed by the National Security Strategy of South Africa, be developed, guided by the JCPS Cybersecurity Response Committee. Level 0

Perceived Capability Rating

Score ■■□□□

South Africa is perceived to be developing offensive cyber capabilities for years now. Progress towards achieving this has largely reported to be negligible. There is no evidence of any offensive cyber capacity, nor attributed cyberattacks to South Africa.

Data availability rating (1 being highest number of sources, 21 lowest): **20/21**

Document	Excerpt
"New players join race for offensive cyber abilities," Oxford Analytica, August 20 2018.	According to the article, "During 2013-15, various media reports based on leaked company documents said that the NCC [National Communications Centre] is a customer of FinFisher, a German cyber surveillance vendor, which among other services, sells interception capabilities." In addition, "South Africa is also developing offensive capabilities under the National Defence Force's Defence Intelligence Division. However, funding shortages in the defence department, due to a stagnating economy, have delayed its plans to establish a Cyber Command Centre Headquarters to the April 2019-march 2020 fiscal year." This is common among many African nations where political instability often hampers modernization efforts. Level 2
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	"The Ministry of Defence's cyber responsibilities include support for civilian agencies, defence of military networks, deterrence, and offensive missions to enhance information superiority," (P. 45). Level 2

South Korea

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ■■□□□

Perceived Capability Rating ■■■□□

Organization for Offensive Cyber	National Intelligence Service and Cyber Command (unconfirmed)
National Cyber Power Index (2020)	Ranked 16th overall and 15th when it comes to offence
National Cybersecurity Index (2022)	68.83 (32nd)
Internet Penetration (2020)	97%
Internet Freedom Score	67/100 (Partly free)

Transparency Description

South Korea's scores for the declared and perceived capability rating only differ slightly at the lower-end of the spectrum. South Korea has not officially disclosed to be in possession of offensive cyber capabilities, nor has a dedicated military doctrine or strategy been published. References to offensive capabilities in official documents remain discrete: they remain purely aspirational and mostly focused on enhancing defence and resilience. However, some sort of offensive capability by South Korea is perceived to exist, especially in consideration of the malicious operations carried out by North Korea. In this regard, sources recently reported that South Korea possesses substantial military cyberspace capabilities and that its deterrence posture against North Korea is likely to extend to cyberspace and cyber operations. As for offensive operations, one APT active since 2007 having reportedly carried out multiple attacks against industries in several countries has been affiliated to the National Intelligence Service (NIS) of South Korea.

Declared Capability Rating

Score ■■□□□

The once passive South Korean cyber defence posture has, in response to North Korean cyber operations, shifted to an acknowledgement of the importance of developing offensive cyber capabilities as a countermeasure. Capabilities are likely to exist but remain unconfirmed by official sources. No further details about the general command structures, conditions of employment or overall principles of operation are disclosed, nor has it published a dedicated cyber defence strategy or doctrine.

Data availability rating (1 being highest number of sources, 10 lowest): **3/10**

Document	Excerpt
"National Cybersecurity Strategy," National Security Office, 2019.	Under the objective of enhancing Cyber Attack Response Capabilities, the National Security Strategy includes the objective to "train cyber warfare specialists and foster response organizations in order to efficiently conduct cybersecurity activities" (P.17) **Level 0**
"2018 Defense White Paper," 2018.	The defence paper does not explicitly mention that South Korea is seeking to obtain offensive cyber capabilities. However, it does hint at it numerous times. For instance, "The ROK Armed Forces aims to build a military power capable of flexible response to omnidirectional security threats including those from North Korea and other potential threats...The ROK Armed Forces will also build the capabilities and systems for effective response to cyber and space threats," (P. 47); "The ROK Armed Forces will use combined and joint forces to conduct simultaneous and integrated operations in all domains, including ground, sea, airspace, and cyber, and thus seize the initiative at the earliest stages of war and achieve a decisive victory in a short period." (P. 65); At one point the Koreans admit to having, and then misusing, their cyber capabilities: "In 2010, the ROK Armed Forces established ROK Cyber Command to form the institutional and organizational basis to conduct cyber warfare. Since then, the ROK Armed Forces has actively responded to the growing cyber threats. However, concerns over the national defense cybersecurity were raised following defense network hacking incident and the controversy over the Cyber Command's unlawful political interference in 2016." (P. 77); "The MND has chosen and implemented the "national defense cybersecurity capability enhancement plan" as a task of "Defense Reform 2.0" to restore the people's trust in the ROK Armed Forces and drastically strengthen the cyber capabilities of the ROK Armed Forces." (P. 78). **Level 1**

Document	Excerpt
"Military Cyber Command to terminate "cyber psychological warfare" operations," Park Byong-su, August 10, 2018.	"We will be moving forward with devising ways to strengthen our cyber security capabilities for national defence, which we have selected as one of the tasks for national defence reform. We are planning to focus on ten major action plans, which include a wholesale reorganization of the Cyber Command's missions and functions," the Defence Ministry said in a document issued on Aug. 9. According to the details of this plan, the Cyber Command will no longer be involved in cyber psychological warfare." Level 1
"National Cybersecurity Strategy (2016)," National Security Office, 2016.	"Despite these efforts, the rapid development of cyberspace and increased threats to cybersecurity demand more proactive attention and action." (P. 8) "However, it is time to further enhance the resilience of national core services and implement active response measures to evolving cyber attacks." (P. 8) Level 1
"Defense White Paper 2016," Ministry of National Defense, December 31 2016.	"Efforts have been dedicated to developing core cyberwarfare technologies while rapidly integrating commercial information security technologies and systems to the defense sector." (P.78) Level 2
"South Korea Seeks Offensive Cyber Capabilities," Zachary Keck, October 11, 2014.	"We will change what has so far been a passive-defensive policy into a proactive one. Taking advantage of the enemy's vulnerabilities, we will take preemptive action to fend off cyberinfiltrations." [unnamed Defence Ministry official, 2014]. Level 1
"South Korea's strange cyberwar admission," Joe Boyle, March 2, 2014.	"South Korea defence chiefs broke those unspoken rules on 19 February by outlining their aim to develop a cyber-tool aimed specifically at knocking out North Korea's nuclear capabilities, according to Yonhap news agency. Their blueprint appears to be a 2010 cyber-attack on Iran, which used software known as Stuxnet to damage nuclear facilities." Level 1
"S. Korea pushes to develop offensive cyberwarfare tools," Kim Eun-jun, February 19 2014.	"South Korea will push to develop sophisticated cyberwarfare tools that could wreak havoc on North Korea's nuclear facilities as part of its plans to beef up offensive capabilities, the Defence Ministry said Wednesday ... The ministry reported a long-term plan for cyberpolicy to the parliamentary defense committee...A strategic plan for the second phase calls for developing cybertools for offense like Stuxnet, a computer virus that damaged Iran's uranium enrichment facility, to cripple North Korea's missile and atomic facilities... "Once the second phase plan is established, the cyber command will carry out comprehensive cyberwarfare missions," a senior ministry official said, asking for anonymity." Level 1

Perceived Capability Rating

Score ■■■□□

South Korea's deterrent against North Korean aggression is perceived to extend into cyberspace. It is seen as having increased investments in its offensive cyber programme, past operations were mostly focused on espionage or information operations, and one APT was linked to its intelligence service.

Data availability rating (1 being highest number of sources, 21 lowest): **13/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	South Korea is ranked as the 16th most comprehensive cyber power and 15th (out of 30) for offensive cyber capabilities.
APT-C-06 (aka DarkHotel, SIG25, Dubnium, Fallout Team, Shadow Crane, ATK 52, Karba, Luder, Nemim, Pioneer, Tapaoux, CTG-1948, TUNGSTEN BRIDGE) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The APT, active since at least 2007, has been affiliated to the National Intelligence Service (NIS) of South Korea. The group carries out cyber espionage attacks directed at multiple industries in a number of countries, notably North Korea, Russia, South Korea, Japan, Bangladesh, Thailand, Taiwan, China, the United States, India, Mozambique, Indonesia and Germany. In 2010, the APT carried out Operation DarkHotel targeting CEOs doing business in the APAC region. Something characteristic about this group is that they are able to track their targets as they travel around the world through hotel Wi-Fi infrastructure. In a depart from their traditional corporate targeting, the 2016 Operation Inexsmar was directed at political figures. In 2018, the group utilised an Internet Explorer vulnerability to gain control of users devices by redirecting them to malicious websites. In 2020, the group targeted Chinese institutions abroad and institutions in Shanghai and Beijing. Level 3

Document	Excerpt
"Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike," Raphael Satter, Jack Stubbs, Christopher Bing, March 23 2020. (1) "An Elite Spy Group Used 5 Zero-Days to Hack North Koreans," Andy Greenberg, March 26 2020. (2)	There are two cyberoperations attributable to the South Koreans. One, a spear phishing attack directed at World Health Organisation employees (1). The other, a sophisticated espionage campaign against North Korea (2). **Level 3**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The book lists South Korea as one state "considered possessing substantial military cyberspace capabilities and some of these countries have announced intentions to create cyber commands and/or cyberattack capabilities," (P. 188). **Level 3**
"The Dyadic Cyber Incident and Dispute Data, Versions 1, 1.1, and 1.5," Ryan C. Maness, June 1 2019.	Lists several cyberattacks from South Korea against Japan, which largely occurred during a dispute over islands. It consists of mainly retaliatory attacks for Japanese DDoS attacks. **Level 3**
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	Given the general threat of North Korea and their cyberattacks, South Korea is very cognizant of the cyber domain. Consequently, "Since 2009, Cyber Command has doubled in size and received an increase in funding of almost 50%." (P. 77). Because of the looming security threat, "The military has a significant and clearly defined role in cyberspace, but its focus remains narrowly on defending against the North Korean threat. Broadening its military narrative to a more comprehensive posture in cyberspace would indicate greater cyber maturity." (P. 77). **Level 3**
"Cyberwarfare in the Korean Peninsula: Asymmetries and Strategic Responses," Nir Kshetri, July 22 2014.	In regard to South Korea's offensive activities, the paper notes the development of cyber-weapons that can "be deployed to physically damage North Korean nuclear plants and missile facilities. South Korean Defence Ministry has announced its intention to develop weapons similar to Stuxnet, which was designed to destroy Iran's nuclear enrichment facilities," (P. 184). In fact, South Korea and the USA also have a close partnership in cyber operations. They've worked together to develop offensive cyber capabilities, and also occasionally conduct cyber warfare exercises together. (P. 193-194). The article notes that South Korea has already conducted a variety of psychological warfare activities against North Korea via their cyber capabilities. (P. 186). Notes that South Korea "Plan to train 5,000 cyber security experts by 2017." (P. 186). **Level 3**
"Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014.	In one instance, South Korea was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	South Korea considers cyberspace to be "an operational domain, such as land, air, and sea, which thus needs a state level defence system. The strategy will focus on defence, i.e., prevention and detection of, and response to cyberattack." (P. 41). As such "The Ministry of National Defence has (...) created an independent Cyber Warfare Command responsible for defensive and offensive operations in cyberspace, (P. 41). In the future "The Republic of Korea also plans to develop offensive and defensive cyberwarfare weapons, and increase manpower in the Cyber Warfare Command (...)to 1,000." (P. 42). **Level 2**

Spain

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber (2022)	Joint Cyberspace Command
National Cyber Power Index (2020)	Ranked 12th overall and 5th when it comes to offence
National Cybersecurity Index (2022)	88.31 (8th)
Internet Penetration (2020)	93%
Internet Freedom Score	n/a

Transparency Description

Spain scores considerably higher for its declared capability compared to outside perceptions. It has released significant information regarding its offensive cyber capabilities, as well as having detailed the structure (general order of battle), and the overall principles and operation of its offensive cyber command. In the latter regard, the Joint Cyberspace Command has been established in 2022, and it is tasked with executing military operations in cyberspace. Furthermore, based on the guidelines adopted by the Ministry of Defence in 2018, cyber measures expressly encompass "defence, exploitation, and attack" operations. Despite being vocal about offensive capabilities, Spain is not perceived as having developed high capabilities, despite having been rated fairly high by certain power indexes. Only one cyber-enabled intelligence operations has been attributed to Spain.

Declared Capability Rating

Score

Spain has recently published official documents describing its cyber capabilities, which include an offensive component, military cyber command and its Cyberspace Operation Forces. To this end, general details are available on its offensive cyber command structure (general order of battle) and overall principles of operation.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"Mando Conjunto del Ciberespacio (MCCE)," Ministry of Defence Official Website, last accessed February 2022.	"The Joint Cyberspace Command (MCCE) will plan, direct, coordinate, control and execute military operations in cyberspace, in accordance with the operational plans in force " [Original: El Mando Conjunto del Ciberespacio planeará, dirigirá, coordinará, controlará y ejecutará las operaciones militares en el ciberespacio, de acuerdo con los planes operativos en vigor]. Under the command of the MCCE, the Cyberspace Operation Force (FOCE) will "execute the activities of information gathering, surveillance, reconnaissance and intelligence development of cyber threats and incidents in cyberspace, in coordination with the CIFAS and in matters of military operations also with the MOPS." [Original: Ejecutará las actividades de obtención de información, vigilancia, reconocimiento y elaboración de inteligencia de ciberamenazas e incidentes en el ciberespacio, en coordinación con el CIFAS y en materia de operaciones militares también con el MOPS] and be « responsible for the execution of military operations that ensure the AF's freedom of action in cyberspace, in accordance with the operational plans in force. Within the scope of the aforementioned operations, it is responsible for the operational and technical management of the activities of all the AF Cybersecurity Operations Centers (COCS). It coordinates with the Army, the Navy and the CESTIC the actions it deems necessary in the cyberspace field. When operations are being developed in the electromagnetic spectrum, it will coordinate that the execution of cyber actions is carried out concurrently with these» [Original : será responsable de la ejecución de las operaciones militares que aseguren la libertad de acción de las FAS en el ciberespacio, de acuerdo con los planes operativos en vigor. En el ámbito de las citadas operaciones, dirige operativa y técnicamente las actividades de todos los Centros de Operaciones de Ciberseguridad (COCS) de las FAS. Coordina con los Ejércitos, la Armada y el CESTIC las acciones que considere necesarias en el ámbito ciberespacial. Cuando se estén desarrollando operaciones en el espectro electromagnético, coordinará que la ejecución de las acciones ciber se realiza de forma concurrente con estas.]

Level 4

Document	Excerpt
"National Defence Directive 2020," President of the Government, June 11, 2020.	Relating to the guidelines of the defence policy the directive notes that "In the scenario that includes the national territory and the areas of sovereignty and interest – maritime, air, and those of cyberspace with a defence dimension – Spain will usually act with its own capabilities." (P. 4). Level 0
"Concepto de Ciberdefensa Resumen Ejecutivo," Ministerio de Defensa, September 28, 2018.	This official document approved by the Chief of the Defence provides a guideline to address the development of military capabilities and the organisation of the Armed Forces in Cyberspace. This document could guide the revision of certain Ministry of Defence policies and regulations currently in force. The guideline defines cyberdefence capabilities to include "defence, exploitation and attack" [Original: una definición clara de las capacidades (defensa, explotación y ataque)]. It also notes that the Armed Forces are faced with the challenge of leveraging their existing cyber defense capabilities to "operate continuously, agilely and efficiently in the increasingly demanding operational scenario."[Original: operar de forma continuada, ágil y eficaz en el cada vez más exigente escenario operativo] Level 3
"National Cybersecurity Strategy," National Security Council, December 1, 2017 (1) "National Cybersecurity Strategy," National Security Council, 2019. (2)	The strategy's objective is to "adopt measures to defend Spain's strategic, political and economic interests, in order to prevent, detect and neutralize covert attacks, including those perpetrated from cyberspace by other States, the intelligence services thereof, or by groups or persons, with the aim of illegally obtaining information." Level 0

Perceived Capability Rating

Score ■■□□□

Spain is perceived to be working on obtaining offensive cyber capabilities. However, few results of this investment have been documented. Only one cyber-enabled intelligence operation has been attributed to Spain. It should also be noted that its offensive cyber capabilities have been rated fairly high by certain cyber power indexes.

Data availability rating (1 being highest number of sources, 21 lowest): **15/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	The index ranks Spain as number five for offensive cyber capabilities and is ranked the 12th most comprehensive cyber power.
"Phone of top Catalan politician 'targeted by government-grade spyware'," Stephanie Kirchgaessner and Sam Jones, July 13 2020.	In one instance, Spain was found to have acquired surveillance and intelligence tools from Israeli private company NSO. Level 1
APT (Careto) (aka The Mask, Ugly Face) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	One APT has been affiliated to the Spanish government, though it has been reported that its attacks ceased in 2014. Level 1
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	The analysis notes that Spain began developing military cyber organizations in 2012, and launched their organisation in 2014. (P. 7). It is in 2014 that "Spain for the first time allocated a budget of €2.3 million to enhance its ability to conduct offensive cyber operations." (P. 11). Level 2
"The Mask" Espionage Malware," Schneier on Security, February 11 2014.	The article attributes a seven year long espionage-based cyber operation to Spain: its goal was to steal sensitive information and its "primary targets are government institutions, diplomatic offices and embassies, energy, oil and gas companies, research organisations and activists. Victims of this targeted attack have been found in 31 countries around the world — from the Middle East and Europe to Africa and the Americas" Level 1
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	At the time of publication (in 2011), the document stressed that Spain had no real documented plans for offensive cyber capabilities. However, it also states that "Although it does not lay out principles for pre-emptive or retaliatory action beyond national borders, preventive measures include not only lessening exposure to potential threats but also dissuasion." (P. 46). Level 0

Sweden

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■□□□

Organization for Offensive Cyber (TBE)
Swedish Armed Forces Cyber Defence Units (ITF and 2ITF)

National Cyber Power Index (2020)
Ranked 13th overall and 13th when it comes to offence

National Cybersecurity Index (2022)	84.42 (12th)
Internet Penetration (2020)	94%
Internet Freedom Score	n/a

Transparency Description

Sweden scores considerably higher for its declared capability compared to outside perceptions of its offensive cyber capability. Sweden has openly disclosed to be in possession of offensive cyber capabilities. In several official documents, the government has routinely stressed the importance of developing offensive capabilities in order to enhance cyber resilience. However, no further details regarding the type of capabilities, the general order of battle, the conditions of employment, or the overall principles of operation have been published. Sweden is perceived to possess limited capabilities and only few sources report on its offensive programme. No offensive cyber operation has been attributed to Sweden thus far.

Declared Capability Rating

Score ■■■□□

The general trend in Swedish self-disclosures is to mention the existence of offensive cyber capabilities and what the future plans to strengthen them are. However, no further details are given regarding the type of capabilities, the general order, conditions of employment, or the overall principles of operation.

Data availability rating (1 being highest number of sources, 10 lowest): **7/10**

Document	Excerpt
"Cyber Defence," Swedish Armed Forces Website, last accessed May 2022	"Swedish cyber defence comprises all capabilities as well as offensive and defensive actions that have been taken to defend critical infrastructure." Level 3
"The Swedish Defence Commission's white book on Sweden's Security Policy and the Development of the Military Defence 2021-2025," The Swedish Defence Commission secretariat, May 14 2019.	In the Defence Commission's cyber strategy, the Swedish Armed Forces is "tasked [with] contribut[ing] to the comprehensive cyber defence in the total defence." This implies not only "protecting their own systems" but also bearing responsibility for offensive cyber defence capabilities with the support of and in dialogue with other agencies, particularly the National Defence Radio Establishment (FRA) and the other defence intelligence agencies, as well as the Swedish Security Service. Level 3
"Comprehensive Cyber Security Action Plan 2019-2022," Swedish Civil Contingencies Agency (MSB), March 2019	The action plan talks of strengthening offensive cyber capabilities: "The Swedish Armed Forces with support from the FRA are strengthening the ability to conduct defensive and offensive operations against a qualified opponent in cyberspace"(P.29). This implies that those capabilities already exist, but without going into details or revealing specific details about them. Level 3

Document	Excerpt
"A National Cyber Security Strategy," Ministry of Justice, June 22 2017	The strategy is limited to a description of what the national cyber defence body ought to be: "A national cyber defence presupposes a strong national security service and defence intelligence capability to identify threatening activity, regarding actors and methods, a strong protection of the most security-sensitive societal infrastructures, a high capability to detect, warn of and manage intrusions and attacks, as well as a robust capability to conduct active operations in the cyber environment." (P.18) The strategy mentions "active measures" and "active operations" when referring to offensive operations or capabilities. **Level 3**

Perceived Capability Rating

Score ■■□□□

Sweden's perceived capability remains limited and is based on limited available data. Most observers refer to the fact that the government acknowledged that it is developing offensive cyber capabilities, or to the expertise residing within its intelligence community. However, no offensive cyber operation has been attributed to Sweden thus far.

Data availability rating (1 being highest number of sources, 21 lowest): **18/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Sweden is ranked as the 13th most comprehensive cyber power, and 13th for offensive cyber capabilities.
"Defining offensive cyber capabilities," Tom Uren, Bart Hogeveen and Fergus Hanson, July 4 2018.	The paper notes that "...some smaller nations, such as the Netherlands, Denmark, Sweden and Greece, are also relatively transparent about the fact that they have offensive cyber capabilities." **Level 2**
"The Swedish Kings of Cyberwar," Cyber Security Intelligence, January 23 2017.	The document describes how Swedish experts assisted the NSA in setting up various surveillance efforts on foreign states: "Noting the Swedish spy agency's unusual technical abilities and reputation for secrecy, NSA officials also viewed it as an ideal collaborator on its hacking and cyberwarfare project, called Quantum." It also notes Sweden's recent efforts in developing cyberwarfare capabilities: "the current Swedish government, led by the center-left Social Democrats, has acknowledged that Sweden is pursuing "offensive" cyberwarfare capabilities, which would include hacking, as well as technology to defend against cyberattacks." **Level 2**
"Swedish Military Desires Cyber-Attack Capability," Atlantic Council, October 18, 2013.	The article describes how Swedish reports claimed the Swedish government is planning to develop offensive cyber capabilities. **Level 2**

Switzerland

Cyber Transparency Score Transparent and High Capability

Declared Capability Rating ■■■□□

Perceived Capability Rating ■■■□□

Organization for Offensive Cyber	Cyber Command
National Cyber Power Index (2020)	Ranked 17th overall and joint last when it comes to offence
National Cybersecurity Index (2022)	76.62 (23rd)
Internet Penetration (2020)	94%
Internet Freedom Score	n/a

Transparency Description

Switzerland's score for both the declared and perceived capability rating is identical and in the middle of the spectrum. has officially disclosed to be in possession of offensive cyber capabilities and that its intelligence services are able to carry out offensive cyber operations. Switzerland has also been vocal about its further aspirations to develop more advanced offensive cyber capabilities. Through sanctioned media, member of the Swiss army declared that a new military cyber doctrine is being developed, and a new Cyber Command is in the process of being established to coordinate with the FUB. Simultaneously, regulatory changes have been enacted to broaden the mandate for offensive cyber operations. Switzerland's perceived capabilities correspond to the information publicly disclosed by the government so far, and several sources confirm that Switzerland is increasingly investing in developing offensive capabilities. No offensive cyber operations nor APT has ever been attributed to Switzerland.

Declared Capability Rating

Score ■■■□□

Switzerland has officially acknowledged that its intelligence services can carry out offensive cyber operations, or can ask the military to do so. More recently, a series of new developments have been set in motion that are aimed at improving the Swiss cyber force. This includes regulatory changes to broaden the mandate for offensive cyber operations, the establishment of a Cyber Command next to the FUB, and the development of a military cyber strategy or doctrine.

Data availability rating (1 being highest number of sources, 10 lowest): **4/10**

Document	Excerpt
Führungsunterstützungsbasis (FUB), Schweizerische Eidgenossenschaft, last accessed February 2022.	"FUB acts as a center for electronic operations in the defence against attacks from cyberspace, electronic warfare, and cryptology." Currently, the FUB remains mostly an IT service provider for the Armed Forces, **Level 0**
Interview with Lieutenant General Thomas Sussli, Swiss Cyber Storm, 30 April 2021.	A new general concept for cyber within the armed forces is being developed, which will describe the future cyber capabilities. Simultaneously, a Cyber Command is being established, which will carry out and implement this concept. It is estimated that the Command is operational by January 2024. Until then, cyber operations can be carried out by the intelligence service or they can request the Swiss army, i.e. the FUB's *Zentrum Elektronische Operationen* (ZEO), to carry out an operation. **Level 2**

Document	Excerpt
"Divisionär Alain Vuitel soll Kommando Cyber aufbauen," Von Hans Joerg Maron, March 31 2021.	The article describes the creation of a new Cyber Command. This is to be "developed from the current Armed Forces Command Support Base (FUB) and later become independent." The goal of the Cyber Command is "to be responsible for cyber defence, ICT services, cryptology and electronic warfare from early 2024." The FUB will then "provide the normal information technology services for the military administration." **Level 2**
Revised Swiss Military Law, Government of Switzerland, 2018	The law now allows the military to not only protect their cyberspace but also to conduct offensive cyber countermeasures. **Level 3**
"National strategy for Switzerland's protection against cyber risk for 2018-2022", Schweizerische Eidgenossenschaft, Der Bundesrat, April 2018.	In its objective "to actively counter cyber risks and take the necessary measures to protect the nation's security from threats from cyberspace" (press statement by a Bundesrat delegate, see Netzwoche), the Federal Council has taken measures "to enhance independence and national security and as response to newly emerging cyber threats. However, complete protection against cyber risks cannot be achieved with proportionate measures. Consequently, Switzerland has to increase its resilience to cyber incidents (P. 2) (Original: "Massnahmen müssen getroffen werden, um die Unabhängigkeit und Sicherheit des Landes vor den neu entstehenden oder sich akzentuierenden Bedrohungen und Gefahren im Cyber-Raum zu wahren. (...)Ein vollständiger Schutz vor Cyber-Risiken ist mit verhältnismässigen Massnahmen jedoch nicht erreichbar. Deshalb muss die Schweiz ihre Resilienz gegenüber Cyber-Vorfällen erhöhen.") **Level 0**
"Loi fédérale sur le renseignement," L'Assemblée fédérale de la Confédération Suisse, September 25 2015.	Art. 37 - Infiltration of computer systems and networks 1. If computer systems and networks located abroad are used to attack critical infrastructure in Switzerland, the FIS may infiltrate them in order to disrupt, prevent or slow down access to information. The Federal Council shall decide on the implementation of such a measure. 2. The FIS may infiltrate foreign computer systems and networks in order to search for information that is contained in them or that has been transmitted from them. The Head of the DDPS shall decide on the implementation of such a measure after consultation with the Head of the FDFA and the Head of the FDJP. [Original: Art. 37 Infiltration dans des systèmes et réseaux informatiques. Lorsque des systèmes et réseaux informatiques qui se trouvent à l'étranger sont utilisés pour attaquer des infrastructures critiques en Suisse, le SRC peut les infiltrer afin de perturber, empêcher ou ralentir l'accès à des informations. Le Conseil fédéral décide de la mise en œuvre d'une telle mesure. Le SRC peut infiltrer des systèmes et réseaux informatiques étrangers en vue de rechercher les informations qu'ils contiennent ou qui ont été transmises à partir de ces systèmes et réseaux. Le chef du DDPS décide de mettre en œuvre une telle mesure après avoir consulté le chef du DFAE et le chef du DFJP.] **Level 3**
"National strategy for Switzerland's protection against cyber risks," Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz and Sport VBS, June 19, 2012.	Switzerland sets forth a number of protection measures against cyberattacks: (1) "Crisis Management – Active measures to identify the perpetrator and possible impairment of its infrastructure in the event of a specific threat" (P. 4). According to the document, "there can be no absolute protection against cyber attacks" therefore there is the need for (2) a functioning collaboration of reactive and preventive capabilities are pivotal in order to minimise risks, limit damage and re-establish the initial state of operation of an attacked system" (P. 10). (3)"Each critical infrastructure operator is responsible for his defense. The SRC (Confederation Intelligence Service) can provide assistance in case of cyber attack (if necessary with offensive countermeasures). If the conditions are met, the army may (in the alternative) support it." And (4) the DDPS is responsible for its own defence (if necessary with offensive countermeasures). **Level 3**

Perceived Capability Rating

Score 

The perceived capabilities of Switzerland mostly correspond to external descriptions of the Swiss declared capabilities. Only a handful of report were found that report on Swiss capabilities and no public record of past operations or APTs directly linked to the government.

Data availability rating (1 being highest number of sources, 21 lowest): **18/21**

Document	Excerpt
General Alain Vuitel is to build up Cyber Command, InsideIT, 31 March 2021	"The aim is for the Cyber Command to be responsible for cyber defence, ICT services, cryptology and electronic warfare from the beginning of 2024." Level 2
"Connections National Cyber Defence Policies. Winter 2020," Partnership for Peace Consortium of Defence Academies and Security Studies Institutes, Winter 2020.	The paper explains that a statutory change allowed the Swiss military to partake in offensive cyber activities: "With the revision of the military law, the armed forces can now conduct offensive cyber countermeasures with the authorisation of the Federal Council." (P. 69). As such, the FIS now counts with "the legal basis to conduct offensive cyber countermeasures against infrastructures located outside Switzerland after authorisation by the head of the DDPS who needs to confer with the heads of the FDFA and the FDJP first." (P. 70). Level 3
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Switzerland is ranked as the 17th most comprehensive cyber power and its offensive cyber capabilities as joint last (alongside 13 other states).
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, 2011.	The report states that "The Federal Department of Defence intends to develop cyber defence, exploitation, and attack capabilities." (P. 47). Level 2

Syria

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	15.58 (127th)
Internet Penetration (2020)	36%
Internet Freedom Score	n/a

Transparency Description

A lack of transparency is observed for Syria. While no official indications of offensive cyber capabilities have been disclosed, Syria is largely perceived as possessing some offensive capabilities and carrying out offensive cyber operations. The latter are reportedly supported by the Syrian Electronic Army (SEA), a non-government elite cyber militia. Several APTs, mostly targeting Western media outlets, human rights organisations, communications platforms, and US military websites, have been attributed to the SEA and to Syria.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■■☐☐

Syria's offensive cyber capabilities are perceived to largely reside within the Syrian Electronic Army (SEA) – which is not an official government entity but the nation's loosely governed elite cyber militia that is perceived to be actively backed by the government. It was behind hacks of Western media outlets, human rights organisations, communications platforms, and US military websites. Interestingly, after the SEA disappeared in 2016, it resurfaced a year later in a different form, moving its focus from covert intelligence operations to a public relations extension of the government that seeks to spread disinformation and shape media narratives.

Data availability rating (1 being highest number of sources, 21 lowest): **11/21**

Document	Excerpt
#1 APT-C-27 (aka Goldmouse ATK80, Golden Rat) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	Group attributed to the SEA specialised in information theft and espionage in countries in the Middle East. It was first seen in 2014, the operations usually involve tricking victims into giving away personal information. Level 3

Document	Excerpt
APT (Syrian Electronic Army) (aka SEA, Deadeye Jackal, Syrian Malware Team, ATK 196, TAG-CT2). "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "These hackers are using Android surveillance malware to target opponents of the Syrian government," Danny Palmer, December 10 2018. (2) "Nation-State Mobile Malware Targets Syrians With COVID-19 Lures," Kristin Del Rosso, April 15 2020. (3)	Despite SEA claiming no official standing, experts believe it is affiliated to the Syrian state. It emerged in April 2011 and expressed its support for Syrian President Bashar al-Assad online. The group specialises in information theft, espionage and DDoS attacks against internal targets such as political opposition parties, human rights activists and Syrian website but it is also known for attacking foreign websites in the US, Europe and Middle East. Its most recent operations involve a malware attack to surveil opponents of the Assad regime in 2016 (2) and a surveillance operation using Covid19 as a bait in 2018 (3). **Level 3**
#2 APT-C-37 (aka Pat Bear) "Uncover the Secrets of the Syrian Electronic Army: The role and influence of cyber-attacks in the Syrian Civil War," 360, October 13 2019.	Group attributed to the SEA specialised in information theft and espionage against the "Islamic State". In June 2019, the group launched an information theft attack against Syrian opposition forces. **Level 3**
"Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014.	In one instance, Thailand was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
"Two Members of Syrian Electronic Army Indicted for Conspiracy," US Department of Justice, May 17 2018.	In 2018, the US Department of Justice charged two Syrian nationals for their role in a computer hacking campaign (spearphishing, website defacement, electronic email theft, website redirection and social media hijacking) as members of the SEA. **Level 3**
"The Middle East's Cyber Power: How Syria's cyber war asphyxiated Civil Society Organizations' efforts against the Assad regime," Vinicius Gorczeski, April 2018.	The paper details Syria's usage of cyber weapons against their own populace. **Level 3**
"The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict," Marie Baezner and Patrice Robin, October 2017.	The authors writes: "The leak of Assad's emails in 2012 revealed that the Syrian President received advice from Iran on how to handle demonstrations. Iran is known to have a large cyber branch in the IRGC that may have trained Syrian forces and Hezbollah in Lebanon. It was reported that some members of the IRGC were also integrated in Syrian forces. In October 2013, the commander of the Iranian Cyber War Headquarters was assassinated for allegedly providing support to the SEA. However, misinformation was circulated online about the cooperation between Iran and Syria." (P. 12). **Level 1**
"The Impact of Cyber Capabilities in the Syrian Civil War," Bryan Lee, April 26 2016.	The paper details numerous usages of cyber capabilities by the Syrian government against their own citizens throughout the ongoing Syrian conflict, which included shutting down the internet in parts of the nation. **Level 1**
"Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army," US Department of Justice, March 22 2016.	In 2016, the US Department of Justice indicted three Syrian former or current members of the Syrian Electronic Army (SEA) for their role in the deployment of spearphishing and compromisation of computer systems of the US government and other international organizations, private and media organisations having been antagonistic to the Syrian government. The SEA is not an official government entity but a group of hackers considered to support the Syrian regime. **Level 3**
"Syria: Preparing for the Cyber Threat," Franz-Stefan Gady, September 5 2013.	Back in 2013, in response to American attacks on them, Syria demonstrated some cyber activity by creating some 'cyber angst' in the West through hacking attacks on the private sector. Nevertheless, the article suggests that in the present day "all the open source intelligence gathered at this stage" point towards "Syria's offensive cyber warfare capabilities [being] limited(...)The Assad government's principal focus in cyberspace is domestic." [...] "The Syrian government has little incentive to pour precious resources into sophisticated offensive cyber weapons that will not influence the outcome on the battlefield in Syria." **Level 2**

Thailand

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■☐☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	64.94 (39th)
Internet Penetration (2020)	78%
Internet Freedom Score	36/100 (Not free)

Transparency Description

Thailand's scores for the declared and perceived capability rating differ slightly at the lower-end of the spectrum. Thailand has not officially declared to be in possession of offensive cyber capabilities. However, several sources report on the existence of a Thai cyberwarfare unit, after the Minister of Defence announced in 2015 that such unit would have been created in the upcoming years. Beyond that, no other indication of the unit's structure, rules of engagement, and mandate has ever been disclosed by the government nor reported on by external sources. Thailand's offensive cyber capabilities are perceived as mostly limited to spyware tools used for domestic surveillance operations and censorship. Similarly, Thailand's offensive aspirations remain limited to blocking offensive websites and building resilience against national or international defacements and DDoS attacks.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Document	Excerpt
"Thailand plans new military unit to curb online dissent," News Asia, October 20 2015.	Defence Minister Prawit Wangsuwon told reporters the military is planning to form a unit to fight online dissent. "It's to prevent new types of threats, it's a preemptive measure," he said without elaborating on the nature of the threats." Level 0

Perceived Capability Rating

Score ■☐☐☐☐

Thailand's offensive cyber capability appears to be mostly limited to spyware acquired from foreign vendors for domestic surveillance purposes. Its aspirations are mostly limited to domestic censorship and cyber operations that can support this goal through by defacements and distributed denial-of-service attacks, which are fueled by internal and international political tension.

Data availability rating (1 being highest number of sources, 21 lowest): **18/21**

Document	Excerpt
"Is Thailand's Military Fighting a 'Hybrid War' Threat?" Prashanth Parameswaran, August 13 2019.	"And since coming to power following the 2014 coup, the military has placed an increasing emphasis on threats in the digital domain, including in the cyber realm, perceiving that its opponents are weaponizing these tools for political ends directed at undermining the post-2014 coup regime." **Level 0**
"Champing at the Cyberbit," Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert, December 6 2017.	The report alleges that the Thai army was approached to acquire Cyberbit spyware. **Level 1**
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	The report describes Thailand's cyberwarfare unit: "Thailand's Defence Minister announced in late 2015 that the Royal Thai Armed Forces would be creating a cyberwarfare unit. The unit will comprise members from the three branches of the armed forces and the police force. Its creation was outlined as a priority implementation measure in the armed forces' 2015 five-year plan. Reports vary as to the capability in the unit, but at the very least it seems to possess the ability to block websites deemed offensive and to remediate defacements and distributed denial-of-service attacks fueled by internal and international political tension." (P. 82). **Level 0**
"Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014.	In one instance, Thailand was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**

Turkey

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	Ranked 22nd overall and joint last when it comes to offence
National Cybersecurity Index (2022)	54.55 (57th)
Internet Penetration (2020)	78%
Internet Freedom Score	34/100 (Not free)

Transparency Description

A lack of transparency is observed for Turkey. While having published a number of documents focused on cybersecurity, as well as having announced the development of a Cyber Defence Centre Project (CDCP), no indications of offensive cyber capabilities have ever been disclosed. Indeed, the CDCP is simply tasked with strengthening the Turkish Armed Forces' cyber security and information systems by adopting a "proactive cyber defence capability". Beyond that, Turkey is perceived to possess some form of offensive capabilities and one APT specialised in cyber espionage has been attributed to the Turkish government. Other sources further attributed to Turkey a series of cyberattacks which occurred in late 2018/ early 2019, targeting foreign states with the aim to intercept internet traffic.

Declared Capability Rating

Score ☐☐☐☐☐

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"SSAMER TSK: Cyber Defence Center Project," Presidency of Defence Industries, last accessed February 2022.	The Presidency of Defence Industries, in charge of managing the Defence industry of Turkey and the supply of military technology, is developing a Cyber Defence Center Project: "It was launched with the aim of strengthening the cyber security of TSK's (Turkish Armed Forces) information systems through national software and reducing the possible impact of TSK's cyber incidents by reacting immediately to cyber incidents. The project covers the national development of the cybersecurity software needed and the establishment of a Cyber Defence Operations Center, which ensures that the cyber defence activities carried out within TSK are coordinated from a single point ... the cyber defence operation center was successfully completed in 2017 and put into service of TSK." Level 0
"Turkey's new cybersecurity center to open Monday," Daily Sabah, February 7 2020.	Turkey's National Cyber Response Centre (USOM) is responsible for defensive operations. The center consists of police and gendarmerie officers alongside white-hat hackers. Reports indicate the center will locally develop software to combat cyberattacks but there is currently no evidence to indicate their role in offensive operations. Level 0
"Republic of Turkey Ministry of Transport Maritime Affairs and Communications 2016-2019 Security Strategy," 2016.	"Developing national proactive cyber defence capability for eliminating threats" Level 0
"Important step for cyber army in TSK," Radikal, May 27 2014.	The Turkish Armed Forces specified in a document called "Project Identification Spill" that software and hardware utilized by the Cyber Security Command would be "100 percent national production." The Command "employs close to 30 staff [and] will reportedly be expanded further." The Cyber Command "regularly conducts cybersecurity audits and tests on networks currently used by TSK." Level 0

Document	Excerpt
"Electronic Communications Law," Government of Turkey, November 5 2011.	The authorities and duties of the Ministry of Transport, Maritime Affairs and Communications include "to establish and supervise centers, to produce all kinds of cyber intervention tools and national solutions" [Original: kurdurmak ve denetlemek, her türlü siber müdahale aracının ve millî çözümlerin üretilmesi] Level 0

Perceived Capability Rating

Score ■■■□□

Turkey is recognized to possess some form of offensive capability, albeit often associated with non-state actors that act in the interest of the government. One APT specialised in cyber espionage was also attributed to the Turkish government. Beyond the limited number of reported offensive cyber operations by Turkey, its aspirations to develop these capabilities is also described as being part of its plans to develop a cyber command center.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	Turkey is ranked as the 22nd most comprehensive cyber power and its offensive cyber capabilities are ranked as joint last (alongside 13 other states).
APT (Sea Turtle) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	APT group Sea Turtle has been attributed to the Turkish state. This group has been active since at least 2017 and is specialized in cyber-espionage operations directed at national security organizations, located primarily in the Middle East and North Africa. In 2019, The Institute of Computer Science of the Foundation for Research and Technology – Hellas in Greece announced its networks had been compromised by the group. Level 3
"Exclusive: Hackers acting in Turkey's interests believed to be behind recent cyberattacks – sources," Jack Stubbs, Christopher Bing, Joseph Menn, January 27 2020.	A series of cyberattacks which occurred in late 2018/early 2019 were attributed to Turkey. Many of those affected were foreign states, such as the UK, Iran, and Greece. These attacks involved "intercepting internet traffic to victim websites, potentially enabling hackers to obtain illicit access to the networks of government bodies and other organizations." Level 3
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	The analysis states that "In 2011, Turkey revealed plans to establish a Cyber Command, which was officially established a year later (called the General Staff Warfare and Cyber Defense Command)." (P. 8). Level 2
"A Detailed Look at Hacking Team's Emails About Its Repressive Clients," Cora Currier, Morgan Marquis-Boire, July 7 2015.	In one instance, Turkey was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. Level 1
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	The CSIS report describes the creation of Turkey's Cyber Command: "Turkey merged two agencies in 2010 to create a new entity that is tasked to intercept signals and secure Turkey's electronic communications. It will be staffed by researchers to study cryptography, cybersecurity, electronic warfare, and develop software for the public and private sectors." (P. 48). In the future, "Turkey plans to establish a Cyber Army Command to counter cyberattack against the country, with a special unit within the General Staff to deal with cyber threats." (P. 48). Level 2

Ukraine

Cyber Transparency Score Higher Declared Capability

Declared Capability Rating ■■□□□

Perceived Capability Rating □□□□□

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	Ranked 25th
National Cybersecurity Index (2022)	75.32 (24th)
Internet Penetration (2020)	75%
Internet Freedom Score	62/100 (Partly free)

Transparency Description

Prior to the Russian invasion in February 2022, Ukraine had never declared to be in possession of offensive cyber capabilities. Both the 2016 Cyber Strategy and the 2017 Doctrine of Information Security overtly focused on the enhancement of defensive and intelligence measures to counter threats to the information systems. After the invasion, the Ministry of Defence commissioned a cybersecurity firm based in Kyiv to create a volunteer cyber resistance group that could carry out both defensive and offensive operations against Russia. The establishment of a volunteer cyber group indicates the limited resources that the government is currently able to invest in developing offensive cyber capabilities. Despite routinely serving as the testbed for Russian cyberattacks, Ukraine is not perceived as either possessing or showing aspirations to obtain offensive cyber capabilities. Russian aggression has triggered several responses by Ukrainian Patriotic Hackers to rally around the flag.

Declared Capability Rating

Score ■■□□□

Sanctioned media report on offensive cyber details and/or operations by an official (capabilities are likely to exist but are not confirmed by official resources, and their extent is unknown). Relatively little information was published by the Ukrainian government that disclose any information about their offensive cyber capability. The establishment of a volunteer cyber resistance group in the fight against Russia indicated the limited resources the government has at its disposal.

Data availability rating (1 being highest number of sources, 10 lowest): **8/10**

Document	Excerpt
"EXCLUSIVE Ukraine calls on hacker underground to defend against Russia," Joel Schectman and Christopher Bing, February 25 2022.	Following the advanced Russian invasion of Ukraine from February 2022, Yegor Aushev, the co-founder of a cybersecurity company in Kyiv, was commissioned by the Ukrainian Ministry of Defense to put together a volunteer cyber resistance group in the fight against Russia: "the volunteers would be divided into defensive and offensive cyber units. The defensive unit would be employed to defend infrastructure such as power plants and water systems....The offensive volunteer unit ... would help Ukraine's military conduct digital espionage operations against invading Russian forces." Level 2

Document	Excerpt
"Doctrine of Information Security in Ukraine," President of Ukraine, February 25, 2017. (1) "On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Doctrine of Information Security of Ukraine"," President of Ukraine, 25 February 2017. (2)	Carrying out actions of the intelligence agencies of Ukraine to promote the realisation and protection of Ukraine's national interests in the information sphere, counteracting external threats to the information security of the state outside Ukraine. **Level 0**
"Cyber Strategy of Ukraine (2016)," Ukraine, March 15, 2016.	The Cyber Strategy comprises 3 main objectives: (1)"The establishment and development of tools, means and instruments for potential response to aggression in cyberspace, which can be used as an instrument of military conflict deterrence and military threats prevention in cyberspace." (P. 8); (2) The "Implementation of counterintelligence and operational-investigative measures to combat cyber-terrorism and cyber espionage, as well as assure readiness of critical infrastructure to deal with possible cyberattacks and cyber incident." (P. 5); (3) "Intelligence agencies of Ukraine are to be responsible for: conducting intelligence activities to identify threats to Ukraine's national security in cyberspace, intelligence-gathering operations aimed at other events and circumstances relating to the cyber security matters." (P.5) **Level 0**

Perceived Capability Rating

Score ☐☐☐☐☐

Ukraine's status as a testbed for Russian cyberattacks has encouraged reciprocal attacks by Ukrainian 'Patriotic Hackers,' though the extent to which these groups are related to the state remains dubious. Therefore, Ukraine is perceived to not have acquired or show aspirations to obtain offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 21 lowest): **21/21**

Document	Excerpt
"Cyber Mercenaries and the Crisis in Ukraine," CFR, January 30 2018.	The article describes an interview with Eugene Dokukin, the self-declared commander of the Ukrainian Cyber Forces in which he states the type of operations carried out by the hacktivist group: "activities ranging from the unauthorised monitoring of CCTV cameras and troop movements in eastern Ukraine, to reporting separatist activities to Web companies such as PayPal in an effort to shut down the separatists' accounts, to launching distributed denial of service (DDoS) attacks against websites and leaking sensitive documents from the Russian Ministry of the Interior that revealed details about separatists in eastern Ukraine being paid by Russian authorities." **Level 0**

United Arab Emirates

Cyber Transparency Score Untransparent

Declared Capability Rating

Perceived Capability Rating

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	40.26 (82th)
Internet Penetration (2020)	100 %
Internet Freedom Score	27/100 (Not free)

Transparency Description

A lack of transparency is observed for the United Arab Emirates (UAE). To date, the United Arab Emirates has not officially declared to be in possession of offensive cyber capabilities. This while the UAE is perceived to have acquired spyware tools and other offensive cyber capabilities from foreign vendors. In 2020, Operation Sneaky Krestel was attributed to the UAE. The campaign used NSO Group's Pegasus spyware to hack 36 personal phones belonging to journalists, producers, anchors, and executives of *Al Jazeera*. Beyond that, other sources report that UAE's offensive capabilities may well go beyond the use of spyware tools, and involve malicious operations against regional rivals. In this regard, the UAE has reportedly sponsored the company *DarkMatter* in carrying out hacking and surveillance operations against Qatar.

Declared Capability Rating

Score

No official indications of an offensive cyber capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score

The UAE's offensive cyber capability goes beyond the spyware acquired from foreign vendors and includes offensive operations directed against foreign rivals. The extent of the integration of their capability within the military structure to achieve strategic objectives remains unknown.

Data availability rating (1 being highest number of sources, 21 lowest): **9/21**

Document	Excerpt
"Private Israeli spyware used to hack cellphones of journalists, activists worldwide," Dana Priest, Craig Timberg and Souad Mekhennet, July 18 2021. (1) "Controversial Government Spyware Crops Up in 21 Countries, Report Says," Lorenzo Franceschi-Bicchierai on February 18 2014. (2)	The United Arab Emirates have acquired surveillance and intelligence tools on several occasions, and from various private companies, such as the Israeli NSO and the Italian Hacking Team. Level 1
APT (Stealth Falcon) (aka FruityArmor, Project Raven) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1)	The group, specialised in information theft and espionage against Emirati journalists, activists, and dissidents, was first discovered in 2021. Circumstantial evidence links the attacks to the UAE. Its latest operation in 2019 was against journalists, activists and dissidents in the Middle East. Level 1

Document	Excerpt
"Is the GCC Cyber Resilient?" James Shires and Joyce Hakmeh, March 2020.	The authors note that the UAE has been linked to the purchase of several spyware and other offensive cyber capabilities. (P. 15).Most notably, the document reports that "there are companies in the UAE that blur the lines between offensive capability and benign cybersecurity protection. For example, Dark Matter provides cybersecurity solutions to industry and government, and was reportedly involved in large-scale telecoms interception and targeting of individuals deemed to be a threat. One report, by a former NSA and Dark Matter employee, suggested these targets included US citizens." (P. 16). **Level 1**
"The Great iPwn: Journalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit," Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert, December 2020.	In 2020, Operation "Sneaky Krestel" was attributed to the UAE. The campaign "used NSO Group's Pegasus spyware to hack 36 personal phones belonging to journalists, producers, anchors, and executives at *Al Jazeera*. The personal phone of a journalist at London-based *Al Araby TV* was also hacked." **Level 1**
"Google lets alleged spying app ToTok back into Play Store," Colin Lecher, January 6 2020.	In 2019, a malicious instant messaging app in Google Play Store called ToTok was introduced. According to US intelligence agencies, the app was likely developed by DarkMatter, a hacking company linked to the UAE government and it was used "to try to track every conversation, movement, relationship, appointment, sound and image of those who install it on their phones." **Level 1**
"The Rise of the Rest: Maturing Cyber Threats Beyond the Big Four," Zach Dorfman and Breanne Deppisch, November 2019.	The article comments on UAE's cyber operations against foreign actors stating that "Although all three countries are U.S. security partners, Saudi Arabia and the UAE have acutely antagonistic relations with Qatar, and operations from both sides have targeted the other state or states." It also asserts that "the UAE didn't only use DarkMatter to undertake its covert hacking and surveillance offensive—according to court documents filed in 2018 cited by the New York Times, the NSO group, an Israeli security company with close government ties, also worked with the Emirati government to hack the communications devices of rival foreign government figures." **Level 3**
"Exclusive: UAE used cyber super-weapon to spy on iPhones of foes," Joel Schectman and Christopher Bing, January 30 2019.	In January 2019, "a team of former U.S. government intelligence operatives working for the United Arab Emirates hacked into the iPhones of activists, diplomats and rival foreign leaders with the help of a sophisticated spying tool called Karma." The targets included the Emir of Qatar, a senior Turkish official and a Nobel Peace laureate human-rights activist in Yemen, among others. This allowed the hackers to "obtain photos, emails, text messages and location information from targets' iPhones. The technique also helped the hackers harvest saved passwords, which could be used for other intrusions." **Level 1**
"Inside the UAE's secret hacking team of American mercenaries," Christopher Bing and Joel Schectman, January 30 2019.	The article outlines UAE's cyber espionage efforts and Project Raven where past US intelligence contractor were employed by the UAE to spy on other governments, militants and human rights activists. **Level 1**
"A New Kind of Information Warfare? Cyber-Conflict and the Gulf Crisis 2010-2017," Tarek Cherkaoui, August 2018.	The document assesses UAE's cyber capabilities first notes that the UAE has spent a lot of money purchasing malware for domestic use (P. 12). And moreover suggesting that "the UAE's mass surveillance system was established with the help of an Israeli company." (P. 12). On the UAE offensive capabilities, the report alleges that "the UAE built extensive cyber warfare beyond conventional firepower. The Abu Dhabi authorities chose to work through a new and well-funded private company called DarkMatter." (P. 15). In fact, DarkMatter is thought to hide behind a private sector company front while basically functioning as the UAE's version of the NSA. As a matter of fact, it frequently recruits former American NSA or military members. But although "the UAE has been traditionally sourcing its military equipment and know-how from the U.S., a Russian blueprint seems to have directly inspired UAE cyber warfare capabilities and methods of operation." (P. 16). For instance, the article alleges that "almost every measure that Russia deployed during the annexation of Crimea and the conflict with Ukraine was duplicated in the UAE's hostile move against Qatar." (P. 16). **Level 3.5**
"UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence officials," Karen DeYoung and Ellen Nakashima, July 16 2017.	In 2017, US intelligence services attributed to the UAE "the hacking of Qatari government news and social media sites in order to post incendiary false quotes attributed to Qatar's emir, Sheikh Tamim Bin Hamad al-Thani." "The false reports said that the emir, among other things, had called Iran an "Islamic power" and praised Hamas." This attack had multiple consequences: "Citing the emir's reported comments, the Saudis, the UAE, Bahrain and Egypt immediately banned all Qatari media. They then broke relations with Qatar and declared a trade and diplomatic boycott, sending the region into a political and diplomatic tailspin." US attribution of 2017 Qatar government websites hack to UAE: the Washington Post reports that "The United Arab Emirates orchestrated the hacking of Qatari government news and social media sites in order to post incendiary false quotes attributed to Qatar's emir, Sheikh Tamim Bin Hamad al-Thani, in late May that sparked the ongoing upheaval between Qatar and its neighbors, according to U.S. intelligence officials. **Level 3**

Document	Excerpt
"How BAE sold cyber-surveillance tools to Arab states," BBC, June 14 2017.	UAE was found to have bought cybersurveillance tools from a British/Danish company. **Level 1**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	"In September 2011, the United Arab Emirates launched a cyber operations centre in Abu Dhabi. The centre is a joint effort between the firm Emiraje Systems and Khalifa University and will coordinate with the armed forces. The first phase of the United Arab Emirates Command and Control System was completed in February 2011." (P. 88). It was not specified whether this includes an offensive capability. **Level 0**

United Kingdom

Cyber Transparency Score Somewhat Transparent and High Capability

Declared Capability Rating ■■■■□

Perceived Capability Rating ■■■■■

Organization for Offensive Cyber (2020)	Government Communications Headquarter ; National Cyber Force
National Cyber Power Index (2020)	35.57 (3rd)
National Cybersecurity Index (2022)	77.92 (22th)
Internet Penetration (2020)	95%
Internet Freedom Score	78/100 (Free)

Transparency Description

The UK's scores for the declared and perceived capability rating differ slightly at the higher-end of the spectrum. The UK has disclosed to be in possession of offensive cyber capabilities and is one of the few European nations that published a detailed military doctrine regarding Cyber and Electromagnetic Activities (CEMA). UK strategies have routinely acknowledged offensive cyber capabilities as an integral part of the overall military capabilities, and have further referred to the deployment of offensive means to carry out operations in cyberspace, such as the major cyber-campaign launched in 2018 against ISIS. The latest Cyber Strategy (2022) also emphasises that offensive operations may be used to influence individuals and groups, and to disrupt online and communication systems, as well as physical ones, and several documents revealing the existence of a Joint Threat Research Intelligence Group (JTRIG), tasked with carrying out offensive cyber operations, were leaked in 2014. Several past operations have been attributed to the GCHQ and confidential documents indicate the real extent of the British cyber capability and tools.

Declared Capability Rating

Score ■■■■□

The UK is transparent about the fact that it has offensive cyber capabilities, ranging from tactical Cyber and Electromagnetic Activities (CEMA) to strategic cyber operations. The UK shows highest transparency in the former category (CEMA), for which it published a dedicated military doctrine. The latter category appears to reside in GCHQ. Together with the Ministry of Defence, it jointly runs the National Offensive Cyber Programme, which is reported to have a budget £250 million and a staff of 2,000 in 2018. In 2020, the National Cyber Force was established, while previously the Joint Threat Research Intelligence Group (JTRIG) was known to be GCHQs covert cyber warfare unit.

Data availability rating (1 being highest number of sources, 10 lowest): **6/10**

Document	Excerpt
"National Cyber Strategy 2022," UK Government, December 12 2021.	The 2022 cyber strategy emphasizes the investment in offensive cyber capabilities: "We have invested significantly in our offensive cyber capabilities, first through the National Offensive Cyber Programme, and more recently through the establishment of the National Cyber Force (NCF)" while reiterating the purpose of these operations: "NCF operations can be used to influence individuals and groups, disrupt online and communications systems and degrade the operations of physical systems" in order to support "government priorities relating to national security, economic wellbeing, and ... the prevention and detection of serious crime." For 2025, the UK intends to continue to "develop and invest in our offensive cyber capabilities, through the NCF." These capabilities are to be used "responsibly as a force for good alongside diplomatic, economic, criminal justice and military levers of power." Level 3

Document	Excerpt
"National Cyber Force Explainer," National Cyber Force, December 13 2021.	"The National Cyber Force (NCF) was established in 2020, a partnership between defence and intelligence, it is responsible for operating in and through cyberspace to disrupt, deny, degrade and contest those who would do harm to the UK and its allies, to keep the country safe and to protect and promote the UK's interests at home and abroad...The UK has declared its willingness and ability to use cyber operations as an integral component of its diplomatic, economic and military activities." **Level 3**
"UK launched cyber-attack on Islamic State," BBC News, April 12 2018.	GCHQ confirms UK cyberattack against ISIS: according to the BBC, "the UK conducted a "major offensive cyber-campaign" against the Islamic State group, the director of the intelligence agency GCHQ has revealed". **Level 2**
"Joint Doctrine Note 1/18 – Cyber and Electromagnetic Activities," Ministry of Defence, February 2018.	The Ministry of Defense defines "CEMA (...)as: the synchronisation and coordination of offensive, defensive, inform and enabling activities, across the electromagnetic environment and cyberspace. The definition broadly identifies four activities, which are conducted in the electromagnetic environment (EME), cyberspace, or a combination of both." (P. 13) Throughout the document, offensive operations are clearly defined as one of the four activities the Ministry of Defence carries out in cyberspace. **Level 4**
"National Cyber Security Strategy 2016-2021," HM Government, 2016.	In its cyber strategy, the UK emphasises its offensive cyber capabilities: "We have the means to take offensive action in cyberspace, should we choose to do so." (P. 9) The document recognizes "Offensive cyber forms part of the full spectrum of capabilities we will develop to deter adversaries and to deny them opportunities to attack us, in both cyberspace and the physical sphere." (P. 47) but also mentions "operational purposes, in accordance with national and international law." (P. 51). Finally, the strategy sets out objectives: "The Government will measure our success in establishing offensive cyber capabilities by assessing progress towards the following outcomes: the UK is a world leader in offensive cyber capability; and the UK has established a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities." (P. 51) **Level 4**

Perceived Capability Rating

Score 

The UK is widely regarded to have an advanced offensive cyber programme. Several past operations have been attributed to GCHQ and, following the Snowden leaks, several confidential documents were leaked that indicated the extent of British cyber capability, its tools, and past operations.

Data availability rating (1 being highest number of sources, 21 lowest): **7/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	The UK is ranked number two for offensive cyber capabilities (narrowly behind the US and comfortably in front of Russia) and ranked as the number 3 for most comprehensive cyber power.
"Britain has offensive cyberwar capability, top general admits," Dan Sabbagh, September 25 2020.	"Gen Sir Patrick Sanders, who heads the UK's strategic command, said that he been told by Boris Johnson to ensure Britain is a "leading, full-spectrum cyber power" able both to defend against – and carry out – hacking attacks. But while the British military claims to have had an offensive cyber capability for a decade, it has rarely been publicly discussed. Sanders said the armed forces worked "in partnership with GCHQ" to deliver "offensive cyber capabilities". These could, in theory, Sanders said, "degrade, disrupt and even destroy critical capabilities and infrastructure of those who would do us harm, ranging from strategic to tactical targets" both in isolation or alongside traditional military force." **Level 5**
APT (GCHQ) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "UK launched cyber-attack on Islamic State," BBC, April 12 2018 (2).	Only one APT was identified to be affiliated to the UK government GCHQ, one of the British intelligence agencies. Known operations include the interception of politicians' communications at G20 summits in 2009 and Operation Socialist, a "breach of the infrastructure of the Belgian telecommunications company Belgacom" (1). In 2018, the GCHQ acknowledged carrying out multiple offensive cyberoperations against the Islamic State (2). **Level 3**

Document	Excerpt
"GCHQ and UK Mass Surveillance: Beyond signals intelligence: Offensive capabilities," Open Rights Group, March 5 2020.	The article describes the offensive activities of the GCHQ: "According to the Snowden documents, proactive actions, now represent 5% of GCHQ's [UK's main signals intelligence agency] "business". Some of these actions will involve the hacking and disabling of target systems described in the previous sections. But GCHQ also appears to engage in dirty tricks and psychological manipulation programmes. The unit leading these efforts is called the Joint Intelligence Threat Research Group (JTRIG) with 150 staff trained in online covert operations, which they see as a third pillar of activities complementary to signals intelligence and computer network exploitation." (P. 2). (...)"Besides engaging in psychological warfare and the mass implants of malware, GCHQ has engaged in disabling remote systems through Denial of Service (DOS) attacks. This involves flooding the capacity of a networked computer system until it collapses. According to documents published by NBC, Anonymous' chat rooms were shut down by GCHQ's own hacking operations in 2011, called Rolling Thunder, with the effect of pushing away some 80% of visitors. According to NBC, this is the first time that a Western government has been found carrying that sort of attack, normally attributed to Chinese and Russian covert operations." (P. 3). **Level 4**
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	According to Tikken and Kerttunen (2020)"in the UK and US operational level cyberspace capabilities are integrated with information environment and space-related capabilities. Moreover, the UK and US army doctrines integrate, synchronize, de-conflict, and coordinate cyber operations and electromagnetic activities." (P. 191). **Level 5**
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	The analysis notes that "The UK aims to become "a world leader in offensive cyber capability; and [...] to establish "a pipeline of skills and expertise to develop and deploy our sovereign offensive cyber capabilities"." (P. 8-9). It also mentions that the UK is one of five NATO members willing to contribute national cyber forces to NATO missions and operations. (P. 2). Finally, notes that the UK established and launched a military cyber organization in 2012. (P. 7). **Level 5**
"Britain to increase investment in cyber-warfare capabilities," NCC Group, February 12 2019.	"On cyber, Mr Williamson [UK Secretary of State for Defence] promised to add to the 1.9bn that the government has already committed to improve Britain's offensive and defensive cyber capabilities. This is to be achieved by utilising advanced technologies, enforcing new structures across government, and protecting domestic networks from online attacks." **Level 4**
"Britain used Spy Team to Shape Latin American Public Opinion on Falklands," Andrew Fishman, Glenn Greenwald, April 2 2015.	"Operation Quito," active since at least 2009, is a cyber-enabled influence operation launched by the JTRIG to prevent Argentina from seizing the Falkland islands. It involved "Network Analysis" and most likely other methods such as the ones listed in the documents above. **Level 3**
"Cyber defence in the EU Preparing for cyber warfare?" Carmen-Cristina Cirlig, October 2014.	"The UK announced in 2013 its intention to incorporate cyber warfare as part of future military operations and to develop a 'cyber strike force' to respond to potential military use of cyber capabilities." (P. 8). **Level 4**
"Snowden Docs Show British Spies Used Sex and 'Dirty Tricks," NBC News, February 7 2014.(1) "The Snowden Files: British Spies Used Sex and 'Dirty Tricks,' Slideshow No. 1," NBC News Investigations, 2012. (2) "The Snowden Files: British Spies Used Sex and 'Dirty Tricks,' Slideshow No. 2," NBC News Investigations, 2010. (3)	The documents leaked by Edward Snowden in 2014 included classified PowerPoint presentations describing the offensive techniques used by the Joint Threat Research and Intelligence Group (JTRIG) to undermine UK's adversaries. According to the article released by NBC News, "both PowerPoint presentations describe "Effects" campaigns that are broadly divided into two categories: cyber-attacks and propaganda operations... The propaganda campaigns use deception, mass messaging and "pushing stories" via Twitter, Flickr, Facebook and YouTube. JTRIG also uses "false flag" operations, in which British agents carry out online actions that are designed to look like they were performed by one of Britain's adversaries" (1). Cyberespionage operations carried out by the unit include methods like the "Royal Concierge" which "exploits hotel reservations to track the whereabouts of foreign diplomats and send out "daily alerts to analysts working on governmental hard targets" (1). Then the "targets can be monitored electronically – or in person by British operatives" (1). Other operations include "changing photos on social media sites and emailing and texting colleagues and neighbors unsavory information" (1). Some slides show more type of attacks including DDos, masquerading and spoofing (3) **Level 5**
"How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations," Glenn Greenwald, February 25 2014 (1). "The Art of Deception: Training for a New Generation of Online Convert Operations," The Intercept, February 25 2014. (2)	In a new document leaked by Snowden entitled "The Art of Deception: Training for Online Covert Operations," the work of GCHQ's "Human Science Operations Cell" is uncovered: it specialises in "online human intelligence" and "strategic influence and disruption." The slides "under the title "Online Covert Action", the document details a variety of means to engage in "influence and info ops" as well as "disruption and computer net attack," while dissecting how human beings can be manipulated using "leaders," "trust," "obedience" and "compliance"" ... "The documents lay out theories of how humans interact with one another, particularly online, and then attempt to identify ways to influence the outcomes – or "game" it." These include for instance: exploit prior beliefs, create cognitive stress, exploit shared affect, etc. **Level 5**

Document	Excerpt
"Hacking Online Polls and Other Ways British Spies Seek to Control the Internet," Glenn Greenwald, July 14 2014. (1) "JTRIG Tools and Techniques," The Intercept, July 14 2014. (2)	The article reports on the set of tools developed and used by the GCHQ's Joint Threat Research Intelligence Group (JTRIG). According to the article, they constitute "some of the most startling methods of propaganda and internet deception contained within the Snowden archive." Methods of "fake victim blog posts," "false flag operations," "honey traps" and psychological manipulation have been previously reported on. The new leaked document (2) "provides a comprehensive, birds-eye view of just how underhanded and invasive this unit's operations are." Their methods include invasive espionage techniques such as Twitter monitoring and profile collection, IP harvesting, provision of real time call records on Skype and instant messaging, collection of data on Facebook, etc (2). But it also includes effects capabilities like DDos, capability to send spoofed SMS messages, mass delivery of emails to support information operations, masquerading Facebook wall posts for an individual or entire nation, etc. (2). **Level 5**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	The report outlines the funding allocated to UK's National Cyber Programme which amounted to ""£650 million through 2015." It remarks that "Two thirds of this funding will be allocated to developing "operational capabilities", and "20 per cent to public and private critical cyber infrastructure." (P. 50). The organization and tasks of the programme are described as follows: "The updated 2011 Strategy states that the new Joint Forces Command will lead development and integration of cyber defence capabilities. The Strategy also calls for the creation of two Joint Cyber Units... The second unit will be within Government Communications Headquarters, with responsibility to develop "new tactics, techniques, and plans to deliver military effects ... through operations in cyberspace."" (P. 51). **Level 2**
"MI6 Attacks Al-Qaeda In 'Operation Cupcake'," Duncan Gardham, June 2 2011.	Operation Cupcake was launched in 2011 by MI6 and GCHQ to impede al-Qaeda efforts to recruit English-speaking terrorist through a propaganda magazine. The magazine in question originally featured recipes for making homemade bombs. British intelligence hackers inserted into the original magazine code redirecting readers to a web page with cupcake recipes. **Level 3**

United States

Cyber Transparency Score Transparent and High Capability

Declared Capability Rating ■■■■■

Perceived Capability Rating ■■■■■

Organization for Offensive Cyber	Department of Defense (US Cyber Command in particular) and intelligence services (NSA in particular)
National Cyber Power Index (2020)	50.24 (1st)
National Cybersecurity Index (2022)	79.22 (21st)
Internet Penetration (2020)	91%
Internet Freedom Score	75/100 (Free)

Transparency Description

The United States is by far the dominant cyber superpower and has shown the highest transparency in its offensive cyber capabilities. JP 3-12 (cyber operations) and FM 3-12 (CEMA) describe in detail the planning and execution of cyber operations, including a description of the types of effects, order of battle. Offensive operations are conducted by the intelligence community (National Security Agency, in particular TAO) and the Department of Defence (DoD), the cyber branches of the Army, Navy and Air Force, and the recently established Cyber Command (US CYBERCOM). The U.S. is unanimously regarded as the world's leading cyber power with an unmatched offensive cyber programme that has the proven capability to degrade and destroy enemy systems and infrastructures. Widely regarded as the cyber superpower, "only" fourteen offensive cyber operations have been attributed to the U.S., including several prominent operations such as *Stuxnet* in 2010 and the 2016 attacks against ISIS.

Declared Capability Rating

Score ■■■■■

The United States remains the preeminent cyber super power and shows the highest ranking in terms of its declared capability, most notably by publishing its military cyber doctrines (i.e. JP 3-12 and FM 3-12). Offensive operations are conducted primarily through the National Security Agency (NSA), Department of Defence (DoD), US Cyber Command and the cyber branches of the Army, Navy and Air Force.

Data availability rating (1 being highest number of sources, 10 lowest): **1/10**

Document	Excerpt
"U.S. Army Cyber Command," U.S. Cyber Command, September 2, 2020. (1) "ARMY CYBER FACT SHEET: Army Cyber Command," US Army Cyber Command, October 4 2019. (2)	Their website describes their cyber command, including the size, budget, operational units, and duties (including offensive operations and information warfare.) According to their website, the "U.S. Army Cyber Command integrates and conducts cyberspace, electronic warfare, and information operations, ensuring decision dominance and freedom of action for friendly forces in and through the cyber domain and the information environment, while denying the same to our adversaries." They also list a number of resources outlining the structure and details of the U.S. Cyber Command, including a detailed fact sheet. Level 5
"Opinion: Trump confirms, in an interview, a U.S. cyberattack on Russia," Marc A. Thiessen, July 10 2020. (Interview with Donald Trump)	President Donald Trump confirmed in the interview the US had conducted a covert cyberattack in 2018 against Russia's Internet Research Agency: "Asked whether he had launched the attack, Trump replied: "Correct""... Senior U.S. officials also confirmed for me that the strike occurred and was effective, taking the Internet Research Agency offline...The cyberattack appears to have been the first that was designed to frustrate Moscow's attempts to interfere with a U.S. election." Level 2
"US NDAA 2021," U.S. Congress, January 3, 2020.	The Act details a number of desired expansions to the American cyber programme, as well as the budget of the entire programme. Level 5

Document	Excerpt
"U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," Ellen Nakashima, February 27 2019.	US Cyber Command 2019 operation against Russia: "the U.S. military blocked Internet access to an infamous Russian entity seeking to sow discord among Americans during the 2018 midterms, several U.S. officials said. (...) The strike on the Internet Research Agency (...) was part of the first offensive cyber-campaign against Russia designed to thwart attempts to interfere with a US election, officials said." **Level 2**
"How US Military Hackers Prepared to Hack the Islamic State," Joseph Cox, August 1 2018. (1) "Cybercom Operation Glowing Symphony Documents," US Cyber Command, June 27 2018. (2)	The article describes a 2016 US Cyber Command (CYBERCOM) Operation named Operation Glowing Symphony. The information on the campaign was extracted from top secret documents disclosed through the Freedom of Information Act. "The campaign was focused on disrupting the Islamic State's ability to distribute its propaganda. CYBERCOM hackers obtained the passwords to multiple Islamic State administrator accounts, deleted battlefield footage, and changed the passwords, locking the administrators out." The operation involved "hacking into infrastructure hosted within the borders of allied countries." This raised concerns about having to notify ally countries in order not to undermine cooperation. It is unclear how successful the operation was in disrupting ISIS propaganda. **Level 2**
"National Cyber Strategy of the United States of America," President of the U.S., September 2018.	The strategy outlines that any "Activity that is contrary to responsible behaviour in cyberspace " must be "deterred through the imposition of costs (...) through cyber and non-cyber means". This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities" (P. 3) thus, reinstating that "All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States." (P. 21) **Level 3**
"JP 3-12: Cyberspace Operations," Joint Chiefs of Staff, June 8, 2018 (first edition released in 2013)	This U.S. manual outlines the nature of cyberspace, the organisation and responsibilities of cyberspace operations, and the planning and execution of cyberspace operations as follows: "Commander, United States Cyber Command (CDRUSCYBERCOM), commands a preponderance of the cyberspace forces that are not retained by the Services. USCYBERCOM accomplishes its missions within three primary lines of operation: secure, operate, and defend the DODIN; defend the nation from attack in cyberspace; and provide cyberspace support as required to combatant commanders (CCDRs). The Services man, train, and equip cyberspace units and provide them to USCYBERCOM through the SCCs." (P. I-10). In 2013, JP 3-12 introduced the term "Cyberspace Operations" that employ capabilities "to create effects which support operations across the physical domains and cyberspace," (P. I-5) while information operations employ "information-related capabilities [...] to influence, disrupt, corrupt, or usurp the decision-making of adversaries." (P. I-5) This marked the end of the DoD' conception of cyberspace operations as a subset of IO. **Level 5**
"Summary Department of Defense Cyber Strategy," Department of Defense, 2018.	The summary reinstates the importance of defend forward and persistent engagement strategies for national security: "We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." (P. 1) In the interest of national security: "Our primary role in this homeland defense mission is to defend forward by leveraging our focus outward to stop threats before they reach their targets." (P. 2) **Level 5**
"JP 3-13: Information Operations," Joint Chiefs of Staff, November 20, 2014. (first edition 1998)	The first edition of JP 3-13 was published in 1998 and for many years was the keystone document to understand the US military's overall approach to cyber operations. This publication is a doctrine for the planning and execution of information operations in U.S. military operations. The document states that "When employed in support of IO [information operations], CO [cyberspace operations] generally focus on the integration of offensive and defensive capabilities exercised in and through cyberspace, in concert with other IRCs, and coordination across multiple lines of operation and lines of effort." (P. II-9) **Level 5**
"FM 3-12: Cyberspace and Electronic Warfare Operations," Department of the Army, April 2017 (preceded by FM 3-38, February 2014)	This Field Manual details offensive cyber capabilities that are mostly relevant within the tactical environment of the battlefield that is focused on Cyber and Electromagnetic Activities (CEMA) including definitions of the desired effects, the structure, and the general TTPs. More concretely, it asserts that: "Superiority in cyberspace and the EMS to support Army operations results from effectively synchronizing Department of Defense information network (DODIN) operations, offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), electronic attack, electronic protection, electronic warfare support, and spectrum management operations (SMO)." (P. 1-1) **Level 5**
"Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations," The Secretary of Defense, June 23, 2009.	This document creates the U.S. Cyber Command, noting that "Cyberspace and its associated technologies offer unprecedented opportunities to the United States and are vital to our Nation's security and, by extension, to all aspects of military operations. Yet our increasing dependency on cyberspace, alongside a growing array of cyber threats and vulnerabilities, adds a new element of risk to our national security. To address this risk effectively and to secure freedom of action in cyberspace, the Department of Defense requires a command that possesses the required technical capability and remains focused on the integration of cyberspace operations. Further, this command must be capable of synchronizing warfighting effects across the global security environment as well as providing support to civil authorities and international partners." **Level 3**

Perceived Capability Rating

Score 

The US is perceived as the leading cyber power, with unmatched offensive capabilities residing in the intelligence agencies (i.e. NSA TAO) and USCYBERCOM. It is viewed as having launched several successful offensive cyber operations with the proven capability to denigrate and destroy enemy systems or infrastructure.

Data availability rating (1 being highest number of sources, 21 lowest): **8/21**

Document	Excerpt
"National Cyber Power Index 2020," Belfer Center for Science and International Affairs, September 2020.	The US is ranked as the most comprehensive cyber power. Moreover, the US is also ranked as having the best offensive cyber capabilities. Thus, in both categories, the US is in the top countries. Level 5
"Cyber Operations Tracker," Council on Foreign Relations, 2020.	The database attributes fourteen offensive cyber operations to the US. This includes several prominent offensive operations, including Stuxnet in 2010 and the 2016 attacks against ISIS. Level 5
APT-C-39 (aka Longhorn, The Lamberts, Vault7, PLATINUM TERMINAL) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	Longhorn is behind espionage-type operations in at least 16 different countries, compromising governments and the financial, telecoms, energy, aerospace, education, and natural resources sectors. The group was linked to the CIA in 2017 when some of the group's operations and tools were exposed on WikiLeaks. Level 1
APT (Equation Group) (aka Tilded Team, PLATINUM COLONY) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020.	The group, believed to be tied to the NSA's Tailored Access Operations unit, is behind hundreds, if not thousands, of infections in 42 different countries. Thought to be one of the most sophisticated computer attack groups in the world, it utilises novel and sophisticated malware to infect government and defence sectors as well as infrastructure, media, individuals, and companies. The Equation group is also thought be linked to the 2010 Stuxnet attack. Level 5
"GCHQ and UK Mass Surveillance: Beyond signals intelligence: Offensive capabilities," Open Rights Group, March 5 2020.	"The agencies are also developing cyber-warfare capabilities, with the NSA taking the lead within the US armed forces. This militarisation of the internet saw U.S. intelligence services carried out 231 offensive cyber-operations in 2011." (P. 1). Level 5
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The book states that the US consistently continues to develop its cyber military capabilities. In 2009, "a force goal of 133 teams, comprising of circa 5,000 troops was set." By May 2017 the force achieved a "full operational capability, with circa 6,200 troops" P. 100-101). In May 2018, "the US cyber command announced full operational capability of 133 cyber mission force teams (with an additional 21 teams planned to achieve that milestone in 2024). In the same month, the Command was elevated to a unified combatant command status." (P. 189). In terms of strategy, according to Lewis (2019) President Obama's "legalistic and timid approach" to cybersecurity is "significantly changed under the Trump administration" with the realization that "US's cyber opponents are unlikely to change their behaviour without the imposition of consequences." In its place, the US adopts two new strategies: "persistent engagement" and another of "collective deterrence." (P. 101). Level 5
"US 'launched cyberattacks on Iran weapons' after drone downing," Al Jazeera, June 23 2019.	"US President Donald Trump ordered a retaliatory military attack against Iran after the drone shootdown but then called it off, saying the response would not be "proportionate" and instead pledged new sanctions on the country. But after the drone's downing, Trump secretly authorised US Cyber Command to carry out a retaliatory cyber-attack on Iran, two officials told the Associated Press news agency on Saturday." Level 5
"Iran says it dismantled a U.S. cyber espionage network," Reuters, June 17 2019.	Iran attribution of 2019 cyber espionage campaign to the US: according to Reuters, "The secretary of Iran's Supreme National Security Council, Ali Shamkhani, said on Monday: "One of the most complicated CIA cyber espionage networks that had an important role in the CIA's operations in different countries was exposed by the Iranian intelligence agencies a while ago and was dismantled." Level 1
"NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," Max Smeets, May 2019.	The analysis claims that the US was the first to establish a military cyber organization in the 1980s. Since then, it has been expanding until the present day (P. 7). It is also noted that the US was one of five NATO members contributing national cyber forces to NATO operations. Level 5

Document	Excerpt
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	The report readily gives the US the highest rank (10) of all actors in the Asia-pacific region noting that "In 2016, the US also outlined its policy on cyber deterrence, which notes that it will use all instruments of national power to deter cyberattacks and other malicious acts in cyberspace that threaten the US and its interests, including its military command and control systems. The US is the most forward-leaning nation in discussing the development and employment of its military cyber capabilities, indicating a significant level of confidence in its capability and the frameworks that guide and govern its use. The Department of Defence has requested funding of US$6.2 billion in the 2017 budget and US$34.6 billion for projects requiring funding over the period from 2017 to 2021, but details of how the money will be spent are scarce." (P. 83). **Level 5**
"Here Are All the Sketchy Government Agencies Buying Hacking Team's Spy Tech," Janus Rose, July 6 2015.	In one instance, the US and various of its law enforcement federal agencies were found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**
"The Real Story of Stuxnet," David Kushner, February 26 2013.	"Although the authors of Stuxnet haven't been officially identified, the size and sophistication of the worm have led experts to believe that it could have been created only with the sponsorship of a nation-state, and although no one's owned up to it, leaks to the press from officials in the United States and Israel strongly suggest that those two countries did the deed." **Level 4**
"Cyber Warfare: Critical Perspectives," Paul Ducheine, Frans Osinga, Joseph Soeters, 2012.	Ducheine et al. (2012) argue that US transparency on its defence strategy is a deterrence strategy in itself: "The DoD intends to present its defence strategy as a warning to deter potential adversaries, who should consider the consequences when cyber-attacking the US 'If you shut down our power grid, maybe we will put a missile down one of your smokestacks', a US military official said in the Wall Street Journal." (P. 27). While "the US DoD is very willing to openly share their offensive intentions" they do so "without compromising in detail their tactics, techniques and procedures." (P. 29) since "most offensive cyber weapons – by their nature – can only be used once before the rest of the world will have an adequate answer to these weapons." The authors argue that the US is a leading power in cyber defense, stating as an example the Cyber Command set up in May 2010 by the US and how it "inspired many other nations in the cyber arena to create cyber task forces or cyber commands, such as South-Korea, Norway, the United Kingdom, and the Netherlands." (P. 28). **Level 5**
"Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	In its assessment of the national doctrine and organization, the CSIS observes that "The Cyber Command, established in 2010 and originally responsible for dealing with threats to the military cyber infrastructure, will now have broader national cyber defence responsibilities because of the Presidential Directive. The Command is responsible for both defensive and offensive operations." (P. 53). In addition, the Defense Advanced Research Projects Agency set up in November 2012 has "released a document soliciting research into the conduct of cyberwar, called Foundational Cyberwarfare (Plan X). The document states that," Plan X will conduct novel research into the nature of cyberwarfare and support development of fundamental strategies needed to dominate the cyber battlespace.." (P. 54). **Level 5**
"Iran blames U.S., Israel for Stuxnet malware," CBS News, April 16 2011.	Iranian attribution of Stuxnet cyberattack to the US and Israel: "A senior Iranian military official says experts have determined the United States and Israel were behind a mysterious computer worm known as Stuxnet that has harmed Iran's nuclear program" **Level 5**

Uzbekistan

Cyber Transparency Score Somewhat Transparent and Low Capability

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■☐☐☐☐

Organization for Offensive Cyber	Intelligence service (Uzbek State Security Service)
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	36.36 (87th)
Internet Penetration (2019)	71%
Internet Freedom Score	28/100 (Not free)

Transparency Description

Uzbekistan's scores for the declared and perceived capability rating only differ slightly at the lower-end of the spectrum. To date, Uzbekistan has not officially declared to be in possession of offensive cyber capabilities, nor has it published any strategy or military doctrine in this regard. Uzbekistan's perceived capabilities are limited to surveillance and intelligence tools acquired from foreign vendors and used for domestic purposes. In 2020, an APT known as *SandCat* was deemed to be affiliated with the Uzbekistani government and was directly attributed to the Uzbek State Security Service (SSS). However, the group was perceived to lack basic operational security measures and relied on unsophisticated tools.

Declared Capability Rating

Score ☐☐☐☐☐

No Official Indications of an Offensive Cyber Capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■☐☐☐☐

Uzbekistan's offensive cyber capability appears to be mostly limited to spyware and zero-day vulnerabilities acquired from foreign vendors. APT Sandcat, believed to be the Uzbek intelligence agency, the State Security Service (SSS), is a relatively new APT uncovered in 2019 but is missing basic operational security. Previously its capability was limited to acquiring spyware tools from Hacking Team.

Data availability rating (1 being highest number of sources, 21 lowest): **16/21**

Document	Excerpt
APT (SandCat) "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020 (1) "Threat Groups SandCat, FruityArmor Exploiting Microsoft Win32k Flaw," Lindsey O'Donnell, March 13 2019 (2)	One APT was found to be affiliated to the Uzbekistani government: *SandCat*. Its attacks have been directly attributed to the Uzbek State Security Service (SSS). It was first observed in 2018 but is thought to have been active since before that. It has directed its attacks against victims in the Middle East, especially in Saudi Arabia. Level 1
"Uzbek spies attacked dissidents with off-the-shelf hacking tools," Jack Stubbs and Christopher Bing, October 3 2019.	Karpersky attributed a series of cyber operations against activists and dissidents using German spyware FinFisher to the Uzbek state Level 1

Document	Excerpt
"Kaspersky finds Uzbekistan hacking op... because group used Kaspersky AV," Sean Gallagher, October 3 2019 (1). "Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC," Kim Zetter, October 3 2019 (2).	Uzbekistan appears to have bought zero-days from Israeli companies, made use of them and got caught, causing Western companies to patch up the flaws which made these APTs possible. The article by Vice states that due to the Uzbek SSS' lack of operational security "led Kaspersky to discover four zero-day exploits SandCat had purchased from third-party brokers to target victim machines, effectively rendering those exploits ineffective. And the mistakes not only allowed Kaspersky to track the Uzbek spy agency's activity but also the activity of other nation-state groups in Saudi Arabia and the United Arab Emirates who were using some of the same exploits SandCat was using" (2). Nonetheless, the Uzbek SSS seems to have a considerable budget if they were able to purchase off-the-shelf capabilities from the Israeli firms NSO Group and Candiru. **Level 1**
"Here Are All the Sketchy Government Agencies Buying Hacking Team's Spy Tech," Janus Rose, July 6 2015.	In one instance, Uzbekistan was found to have acquired surveillance and intelligence tools from Italian private company Hacking Team. **Level 1**

Venezuela

Cyber Transparency Score Untransparent

Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■☐☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	n/a
National Cybersecurity Index (2022)	32.47 (97th)
Internet Penetration (2014)	62%
Internet Freedom Score	28/100 (Not free)

Transparency Description

Venezuela's scores for the declared and perceived capability rating differ considerably at the lower-end of the spectrum. Venezuela has not officially declared to be in possession of offensive cyber capabilities so far, nor has it published any strategy or military doctrine in this regard. However, Venezuela is perceived as possessing offensive capability, although mostly limited to spyware tools purchased from foreign vendors. Several sources also reported that Venezuela relies on the expertise of Russia and Cuba for the deployment of cyber capabilities, as alleged by US officials in 2019.

Declared Capability Rating

Score ☐☐☐☐☐

No Official Indications of an Offensive Cyber Capability.

Data availability rating (1 being highest number of sources, 10 lowest): **10/10**

Perceived Capability Rating

Score ■■☐☐☐

Numerous accounts report that Venezuela has shown an interest in obtaining spyware and malware, most likely for domestic purposes. Ties to Cuba and Russia are mentioned for training and developing offensive cyber capabilities.

Data availability rating (1 being highest number of sources, 21 lowest): **19/21**

Document	Excerpt
"The Routledge Handbook of International Cybersecurity," Eneken Tikken and Mika Kerttunen, January 28 2020.	The book suggests that Venezuela has purchased spyware. (P. 67). It also notes that "Neither Russia or China have had particular influence on cybersecurity in the region outside their traditional areas of influence (mostly Cuba and Venezuela)." (P. 242). Level 1
"Russian deployment in Venezuela includes 'cybersecurity personnel': U.S. official," Matt Spetalnick, March 26 2019.	US officials allege that Russia sent a number of cybersecurity experts to Venezuela in 2019. The US believes Russian cybersecurity forces could "be helping Maduro's loyalists with surveillance as well as protection of the government's cyber infrastructure." As a response to the alleged cooperation between both countries "U.S. Senator Bob Menendez, ranking Democrat on the Senate Foreign Relations Committee, sent a letter to Pompeo on Tuesday urging him to determine if Venezuela, Cuba and Nicaragua should face mandatory U.S. sanctions for conducting significant transactions with the Russian defense and intelligence sectors." Level 2
"As cyberwarfare heats up, allies turn to U.S. companies for expertise," Ellen Nakashima, November 22 2012.	The news article alleges that Ecuador and Venezuela have turned to Cuba for help to develop offensive cyber capabilities. According to industry officials, Cuban cyber forces have been trained by top Russian officials. Level 2

Vietnam

Cyber Transparency Score Untransparent

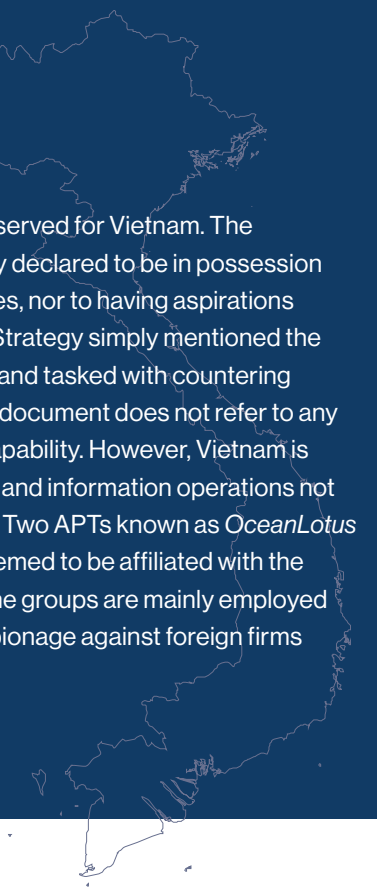
Declared Capability Rating ☐☐☐☐☐

Perceived Capability Rating ■■■☐☐

Organization for Offensive Cyber	n/a
National Cyber Power Index (2020)	Ranked 20th
National Cybersecurity Index (2022)	36.36 (86th)
Internet Penetration (2020)	70%
Internet Freedom Score	22/100 (Not free)

Transparency Description

A lack of transparency is observed for Vietnam. The government has not officially declared to be in possession of offensive cyber capabilities, nor to having aspirations thereof. The 2019 Defence Strategy simply mentioned the existence of a Cyber Command tasked with countering information warfare, but the document does not refer to any detail regarding offensive capability. However, Vietnam is perceived as using spyware and information operations not only for domestic purposes. Two APTs known as *OceanLotus* and *SeaLotus* have been deemed to be affiliated with the Vietnamese government. The groups are mainly employed for information theft and espionage against foreign firms and governments.



Declared Capability Rating

Score ☐☐☐☐☐

Vietnam has not disclosed to obtain or to develop offensive cyber capabilities. Task Force 47 is often described as the new military cyber unit, but it is mostly concerned with information operations to combat domestic online dissent.

Data availability rating (1 being highest number of sources, 10 lowest): **9/10**

Document	Excerpt
"2019 Viet Nam National Defence," Ministry of National Defence, 2019.	The document just mentions the existence of a Cyber Command, which counters "information warfare, cyberwarfare" and safeguards "the Homeland." (P. 86). There is no mention of offensive capabilities or aspirations. Level 0
"Law on Cybersecurity," National Assembly, June 12, 2018.	"Prioritising resources to build a specialised force responsible for the protection of cybersecurity [Cybersecurity Task Force or CTF], and upgrading the capacity of such force and of other organisations and individuals participating in the protection of cybersecurity; and prioritising investment in research and development of science and technology for purposes of protecting cybersecurity. Proactive prevention, detection, ending, fighting, and defeating all acts using cyberspace to infringe national security, social order and safety, or the lawful rights and interests of agencies, organizations and individuals; and readiness to prevent any cybersecurity threat." Level 0

Perceived Capability Rating

Score 

Vietnam's offensive cyber capability is perceived to be mostly focused on spyware or information operations for domestic purposes, although several foreign operations have also been reported. Beyond this purpose, the government does not have more sophisticated capabilities nor does it currently show to heavily invest in such capabilities.

Data availability rating (1 being highest number of sources, 21 lowest): **10/21**

Document	Excerpt
"Cyber Capabilities and National Power," IISS, June 28 2021.	The perception is that Vietnam does not have the capabilities nor the interest (currently) to heavily invest and develop offensive cyber capabilities. **Level 0**
APT 32 "Threat Group Cards: a Threat Actor Encyclopedia," ThaiCERT, July 8 2020. (1) "BMW and Hyundai hacked by Vietnamese hackers, report claims," Catalin Cimpanu, December 6 2019. (2) "Vietnamese Threat Actors APT32 Targeting Wuhan Government and Chinese Ministry of Emergency Management in Latest Example of COVID-19 Related Espionage," Scott Henderson, Gabby Roncone, Sarah Jones, John Hultquist, Ben Read, April 22 2020. (3) "Vietnamese hackers exploited Google Play Store for espionage campaign," Shannon Vavra, April 28 2020. (4) "Lined up in the sights of Vietnamese hackers," BR24, October 8 2020. (5) "OceanLotus: Extending Cyber Espionage Operations Through Fake Websites," Steven Adair, Thomas Lancaster, November 6 2020. (6) "Microsoft links Vietnamese state hackers to crypto-mining malware campaign," Catalin Cimpanu, December 1 2020. (7)	One APT group was found to be affiliated with the Vietnamese government: *APT 32,* also known as *OceanLotus* and *SeaLotus*. It has been active since at least 2013 and is mainly employed for information theft and espionage operations. In 2019, the group targeted BMW and Hyundai to steal corporate proprietary data (2). Most recently, in 2020, multiple attacks were recorded. In April, the group launched a spear phishing campaigns against the Wuhan government and China's Ministry of Emergency Management (3) and uploaded malicious apps to Google store to compromise user's devices (4). In November, the group carried out an espionage campaign directed at Vietnamese dissidents, human rights workers, journalists, and private companies in Germany (5). In November, two operations were recorded. One attacking Vietnamese and Southeast Asian internet users by creating a fake online news outlet with malware (6). Another one infecting French and Vietnamese companies and government agencies with crypto-mining malware (7). **Level 3**
"The Rise of the Rest: Maturing Cyber Threats Beyond the Big Four," Zach Dorfman and Breanne Deppisch, November 2019.	"Offensively, Vietnam's main (and only well-known) state-sponsored hacking group has been dubbed APT32 by industry researchers. Researchers say APT32 boasts impressive in-house capabilities, but – like many state-sponsored hacking groups – primarily relies upon deploying readily available tools, such as Cobalt Strike. According to FireEye, APT32 employs a "combination of custom and open-source tools" to breach companies with ties to the manufacturing, hospitality, and auto industries. They also rely heavily on social engineering tricks, such as targeted spear-phishing attacks, and watering-hole attacks, in which hackers compromise legitimate websites and replace the content with phishing information." **Level 3**
"The Truth About Vietnam's New Military Cyber Unit," Nguyen The Phuong, January 10 2018.	Vietnam's substantial Task Force 47 seems to be set up to for internal control/ stability rather than building capabilities for external cyber warfare. It is "only comprised of purely military officials and military personnel who are already part of the armed forces. They are mostly trained in propaganda and equipped with skills to counter what the regime normally dubs as elements of "peaceful revolution" on the Internet, at the time when influencers are using online channels in widespread fashion in today's Vietnam as is the case in other countries as well." **Level 0**
"Vietnam unveils 10,000-strong cyber unit to combat 'wrong views'," Reuters, December 26 2017.	"Vietnam has unveiled a new, 10,000-strong military cyber warfare unit to counter "wrong" views on the Internet, media reported, amid a widening crackdown on critics of the one-party state." **Level 0**

Document	Excerpt
"Cyber maturity in the Asia–pacific region 2016," International Cyber Policy Centre, September 2016.	Despite Vietnam being regularly mentioned in conversations about offensive cyber power in the Southeast Asian region, the report assigns the nation a rating of 3. The document acknowledges cooperation between Vietnam and South Korea on cybersecurity issues: "In November 2015, the Vietnamese People's Army hosted members of South Korea's Defence Security Command, and cybersecurity training was delivered by South Korean experts. Cooperation on cyber issues is set to continue into 2016." but states that "Beyond moves from the Ministry of Public Security to establish a high command for cybersecurity and information security in 2011, there's been little movement to indicate higher level organisational structures or thinking for cyber issues." (P.87) **Level 0**
Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization," Center for Strategic and International Studies, September 22 2011.	"Viet Nam's Ministry of Public Security has proposed the establishment of a high command to provide electronic and cybersecurity for the military, citing the "eventuality of cyber wars" as a key impetus for a cyber-military organization." (P. 54). **Level 2**

The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl