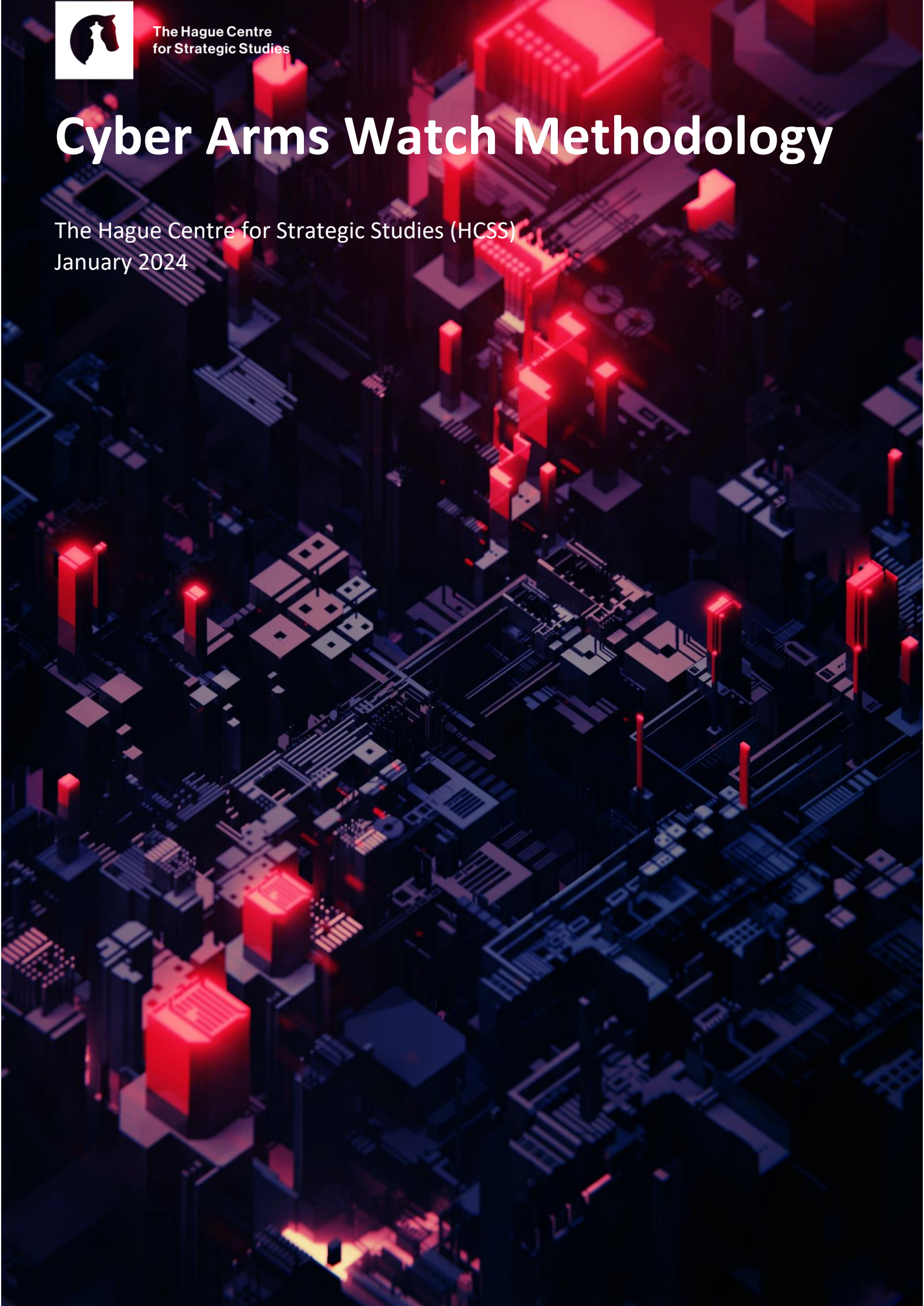
The Hague Centre
for Strategic Studies

Cyber Arms Watch Methodology

The Hague Centre for Strategic Studies (HCSS)
January 2024



Cyber Arms Watch Methodology

Authors: Michel Rademaker, Nino Malekovic, Anna Sophie den Ouden and Nathan Lokhorst.

Review by Charlotte Lindsey (Chief Public Policy Officer, CyberPeace Institute).

January 2024

Cover Image source: Unsplash

This publication is the result of independent research. The responsibility for the content lies entirely with the authors.

HCSS Datalab

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. The frequency, severity, and complexity of cyber operations are on the rise and with state actors are playing a key role in this escalation.[1] According to the Council on Foreign Relations, 48 states are suspected of sponsoring cyber operations since 2005.[2] Despite the high level of activity, relatively little is publicly known about the offensive cyber capabilities of states. Considering that to a defending state, differentiating between immediate preparations for an attack and mere espionage can be challenging, countries might misinterpret the underlying intents of cyber intrusions,[3] risking unintentionally becoming entangled in a cycle of escalation.[4] Avoiding "inadvertent escalation" – or accidental war – remains the most significant challenge between states in cyberspace.

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.[5] 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. To mitigate the dangers of unchecked proliferation and escalation, it's essential to establish more common ground for international discussions on offensive cyber capabilities.[6]

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] Mariarosaria Taddeo, 'Deterrence and Norms to Foster Stability in Cyberspace', *Philosophy & Technology* 31 (10 August 2018): 324, https://doi.org/10.1007/s13347-018-0328-0.
[2] 'Tracking State-Sponsored Cyberattacks Around the World', Council on Foreign Relations, accessed 2 January 2024, https://www.cfr.org/cyber-operations.
[3] Daniel Moore, *Offensive Cyber Operations: Understanding Intangible Warfare* (Oxford University Press, 2022), 23, https://doi.org/10.1093/oso/9780197657553.001.0001.
[4] Alexander Klimburg and Louk Faesen, 'A Balance of Power in Cyberspace', in *Governing Cyberspace: Behavior, Power and Diplomacy*, ed. Dennis Broeders and Bibi van den Berg (London: Rowman & Littlefield International, 2020), 149.
[5] Alexander Klimburg and Louk Faesen, 148.
[6] 'Cyber Capabilities and National Power: A Net Assessment' (The International Institute for Strategic Studies, June 2021), 7, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf.

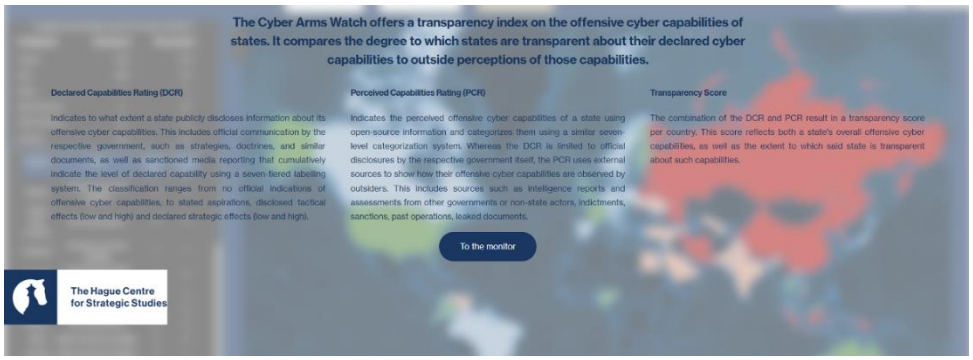
2. Objective: A Cyber Transparency Index

The Cyber Arms Watch aims to contribute 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 55 states. Inspired by the Freedom House Index, the results are visualized as an interactive world map monitor, offering diplomats, academics and researchers alike a one-stop 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.[7] Clicking on a country on the map generates a box indicating the country and its associated country level score and analysis.



In the declared and perceived capabilities tabs, hoovering over the countries on the map will also show the number of documents. At the bottom of the country boxes generated when clicking on a country on the declared and perceived capabilities tabs, a data availability ranking that ranks countries from 1 to 11 (1 representing the largest dataset, 11 the lowest) can be found. The country box includes a 'document' button which leads to a list of data sources used to determine the scorings if clicked on.

[7] 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 0-6, 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 establishing and comparing the results of 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 seven-tiered labelling system (see Table 2). The classification ranges from no official indications of offensive cyber capabilities, to stated aspirations, disclosed tactical effects (low and high) and declared strategic effects (low and high).
>
> **The Perceived Capabilities Rating (PCR)** indicates the perceived offensive cyber capabilities of a state using open-source information and categorizes them using a similar seven-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.

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 6 and PCR of 6, the delta is equal to 0 and indicates transparency. However, the condition of equality should be differently understood between states. Argentina has a DCR of 1 and PCR of 1, so also has a delta of 0. Whilst both the United States and Argentina 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. Which 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.

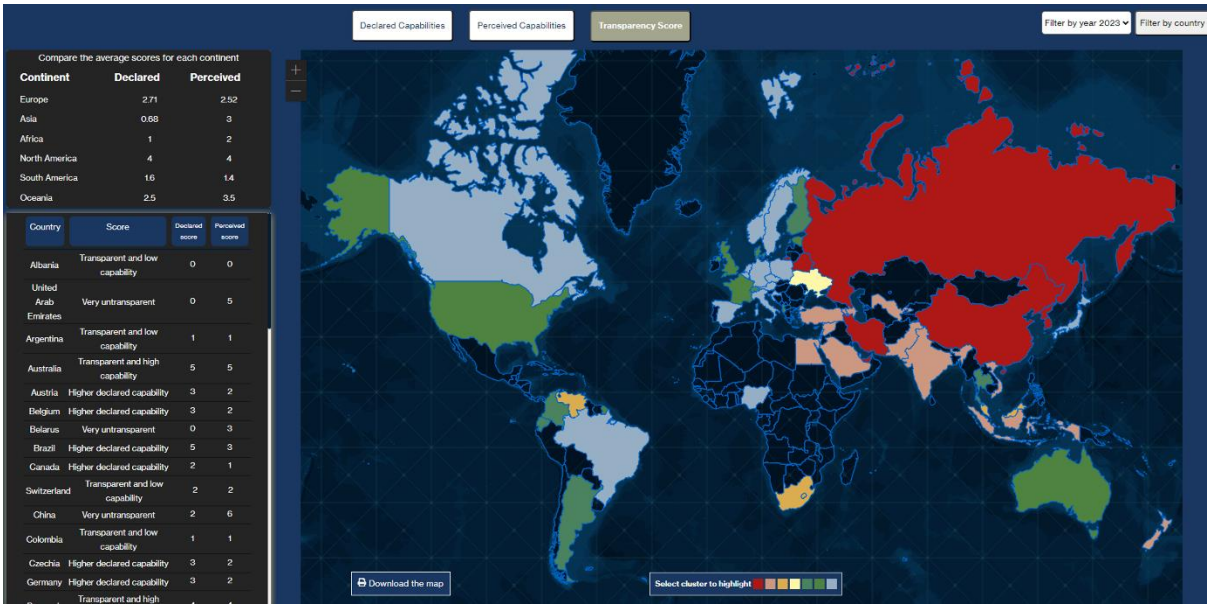


Figure 1: Visualization of the results of the Cyber Transparency Index.

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 sources 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 in the future. The methodology for compiling the underlying database relies on the labelling of publicly available sources according to a seven-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.

Level	Abstract	Declared Capabilities Rating (DCR)	Perceived Capabilities Rating (PCR)
0	Nothing	No official indications of Offensive Cyber Capability	No aspirations to obtain offensive cyber capabilities
1	Aspirations	Stated aspiration for offensive cyber capability	Perceived to be working on obtaining offensive cyber capabilities
2	Emerging capabilities	Some form of offensive capabilities mentioned in national documents or sanctioned media, but details are not disclosed.	Perceived to have developed some form of cyber capability, but details are missing. Furthermore, these capabilities cannot be linked to the military structure.
3	Low tactical effects	Disclosed the use of offensive cyber at the tactical unit level, including CEMA, but does not offer insights into methods, missions or conditions of employment.	Perceived to possess offensive cyber capabilities at the military tactical level, but no evidence of cyber effects is displayed.
4	High tactical effects	Provides details on used methods and effects of offensive cyber at the tactical level, including CEMA. Can also include transparency on military exercises at the tactical level.	Perceived to have integrated offensive cyber capabilities at the tactical level of its military structure and use these capabilities either in exercises or operations.
5	Low strategic effects	National documents which mention a designated unit integrated within the military structure specifically tasked with cyber operations beyond the tactical level, e.g. a cybercommand. Specific details on size or capabilities are not provided.	Perceived to have integrated offensive cyber capabilities into their military structure at the strategic level, but no evidence of attribution to offensive cyber operations is displayed. Can also be perceived to have developed 'branched-in' spyware and used it against foreign actors for strategic purposes.
6	High strategic effects	National documents which mention a designated unit integrated within the military structure specifically tasked with cyber operations beyond the tactical level, e.g. a cybercommand, with specific details on size and capabilities or conducted operations.	Perceived to have integrated offensive cyber capabilities into its military structure at the strategic level with evidence of strategic cyber operations being linked to it.

Table 1: The seven-tiered labelling system for the Cyber Arms Watch.

The included cyber capabilities range from aspirational to tactical to strategic. The tactical-strategic distinction was adopted as throughout the literature, this is the pathway the development of offensive cyber capabilities is perceived to follow, with the states aiming to achieve the end-state of bringing about strategic effects in the cyber domain, be it as deterrent or through action.[8] Offensive cyber capabilities are initially developed at the unit level, supporting kinetic operations, i.e. tactical. Attaining tactical cyber capabilities is less difficult than acquiring some form of strategic effect. Therefore, states that possess a cyber unit that is designated to bring about strategic effects, or is perceived too, can be considered as possessing a higher capability than states which effects are limited to the tactical domain. The distinction between 'low' and 'high' effects was made to create more nuance in the acquired documents. In general, whereas 'low' effects are only stated or perceived, 'high' effects include evidence of actual operations having taken place, be it in the form of exercises or other military action.

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.

States' rating

In establishing the total rating of a country's capabilities (either DCR or PCR), the highest labelled available document is taken as a benchmark. As the labelling system is structured in such a way that the ascending levels build upon each other, the highest labelled available document is a good indicator for a country's overall score. Taking the highest available level as a benchmark is often representative, as a higher-level capability is often preceded by lower levels. Using the highest available level as representative of the overall rating should be seen as a benchmark, not as a hard rule, as there are exceptions. Therefore, there can be cases in which the overall rating of a country is lower than the highest labelled available document. Note that the deviating from the benchmark due to the author's appreciation is the exception, not the rule.

[8] See for example: Daniel Moore, 'Virtual Victory, Applied Cyber Strategy', in *Offensive Cyber Operations* (Oxford University Press, 2022), 101–16, https://academic.oup.com/book/44042; Leonard Spector, 'Cyber Offense and a Changing Strategic Paradigm', *The Washington Quarterly* 45, no. 1 (25 April 2022): 38–56, https://doi.org/10.1080/0163660X.2022.2054123; Max Smeets, 'The Strategic Promise of Offensive Cyber Operations', *Strategic Studies Quarterly* 12, no. 3 (2018): 90–113; Michael Fischerkeller, 'Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies', *Survival* 59, no. 1 (31 January 2017): 103–34, https://doi.org/10.1080/00396338.2017.1282679.

5. Limitations

The Cyber Arms Watch is the first monitor of its kind that aims to measure the extent of nations transparency with regard to their offensive cyber capabilities. These capabilities are some of 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 considered.

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.[9] 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.

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."[10] The issue is simply that they can cover the entire gamut of overt and covert action in cyberspace, meaning that virtually nothing is excludable. 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 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 in the Cyber Arms Watch cover that wide range of cyber operations ranging from the low tactical level to the high strategic. At the tactical level, battlefield cyber capabilities that are sometimes called Cyber Electro=Magnetic Activities (CEMA) were included. It is recognised that offensive cyber is mostly used to deliver an effect (formally known as Computer Network Attacks or CNA) rather than those intended to gather intelligence (formally known as Computer Network Exploitation or CNE). Our declared capability rating follows this logic by excluding cases that revolve around intelligence or influence operations.

[9] Alexander Klimburg and Louk Faesen, 'A Balance of Power in Cyberspace', 148.
[10] 'Cyber Capabilities and National Power: A Net Assessment', 5.

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.

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 capabilities with a perishable and invisible means, 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." [11]

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.

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.

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.

[11] 'Cyber Capabilities and National Power: A Net Assessment', 4.

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 cyberspace, 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. This includes *delegation, orchestration, or sanctioning*.[12] 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.

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

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.[13] 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.[14] 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.[15]

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 spread disinformation and shape media narratives.[16] Russia is described as a country that uses both orchestration and sanctioning in its relations to proxies.

[13] Ibid.
[14] 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".
[15] Global Commission on the Stability of Cyberspace, "Additional Note to the Norm against Offensive Cyber Operations by Non-State Actors," (November 2018).
[16] 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).

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.[17] 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.[18] After all, it offers the Russian government a degree of plausible deniability as it hides behind criminal actors.[19] 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.[20]

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.[21] 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.

[17] 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).
[18] Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (Prentice Hall Press, 2017).
[19] 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).
[20] Mark Galeotti, "Putin's hydra: Inside Russia's intelligence services", European Council on Foreign Relations, (May 11, 2016).
[21] Alexander Klimburg, *The Darkening Web: The War for Cyberspace*, 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. They offer some 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/**.

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**.

HCSS Datalab