Conflict in Cyberspace

Global Security Pulse, Strategic Monitor 2019–2020

The Hague Centre for Strategic Studies

Clingendael — Netherlands Institute of International Relations

Novel and Important Signals to Watch: Threats and Opportunities

- **Malicious actors' probing of the global Domain Name System infrastructure is on the rise**
    - Recent breaches of the DNS, such as 'DNSpionage' (Nov. 2018) and the Netnod attack (Dec. 2018 - Jan. 2019), highlight the international repercussions of exploiting vulnerabilities within critical internet infrastructure. Krebs on Security; TechCrunch
    - The Netnod attack is similar to the Dutch DigiNotar breach (Aug. 2011) in terms of suspected perpetrators (Iranian) and their intent (espionage). Wired; ArsTECHNICA
    - *What further actions can the Netherlands take to deter malicious actors from exploiting critical internet infrastructure?*

- **Economic cyber espionage remains an omnipresent threat to countries' national and economic security**
    - After a short hiatus, Chinese cyber espionage geared toward stealing Intellectual Property (IP) and advanced military technology is on the rise again, as US-China relations deteriorate. NYT (1); NYT (2)
    - Russia and Iran are also conducting cyber-enabled economic espionage operations. Associated Press; The Diplomat
    - Cyber espionage and other cyber crimes are estimated to cost the EU economy €55 billion annually. ECIPE
    - *How can the effectiveness of existing bilateral and multilateral agreements against IP theft be bolstered?*

- **Companies that have suffered a cyber attack are increasingly resorting to offensive action against the perpetrator**
    - "Hack-backs" are part of a self-help strategy that moves away from defensive measures in favor of more offensive options. CFR (1); The New Yorker
    - While norms prohibiting private sector hack-backs are being introduced, a bill before the US Congress would allow limited hack-backs by companies. US Active Cyber Defense Certainty Act; GCSC
    - *How should the Netherlands contribute to an international discussion on this issue?*

- **The US, Russia and China are employing sophisticated forms of Electronic Warfare to maintain military dominance**
    - China modernized its electronic warfare (EW) capabilities, thus allowing them to manipulate access to the electromagnetic spectrum, which includes radio, infrared or radar signals. C4ISRNET; NYT (3)
    - Russian EW capabilities go beyond traditional tactical anti-A2/AD or SEAD by integrating them with cyber and psychological operations (such as degrading the morale of Ukrainian troops in the Dombass). ICDS; OSCE; Business Insider
    - *Are NATO's concepts and practices equipped to respond to adversaries' active combination of EW, cyber- and information warfare?*

Conflict in Cyberspace

Global Security Pulse, Strategic Monitor 2019–2020

The Hague Centre for Strategic Studies

Clingendael — Netherlands Institute of International Relations

Long-Term Trends: Conflict in Cyberspace

Multi-factor Trend Assessment (10-year timespan)

Trends		Trend
Intention	States disclosing offensive cyber capability to enhance transparency	▲
	Perceptions of interstate escalation of tensions in cyberspace	▲
Capacity	Cyber military spending	▲
	National cybersecurity & counter cybercrime spending	▲
Activity	Reported Cyber Enabled Espionage (CNE)	▲
	Reported Cyber Enabled Attacks (CNA)	▲
	Disinformation campaigns	▬

▲ Increase
▬ Stable
▼ Decrease

🟥 Increase threat
🟩 Decrease threat

Conflict in Cyberspace

Global Security Pulse, Strategic Monitor 2019–2020

The Hague Centre for Strategic Studies

Clingendael — Netherlands Institute of International Relations

Novel and Important Signals to Watch: The International Order

- **5G has moved to the forefront of the US-China trade war, leaving Europe in a difficult geopolitical position in the race to Industry 4.0**
    - Huawei is considered an extension of the Chinese state, thereby expanding the ability of China to penetrate telecommunication systems for malicious cyber activity. CCDCOE; Forbes (1); Forbes (2)
    - In Europe, governments appear to allow partial access of Huawei to its telecommunication infrastructure, enhancing geo-political tensions with the US. Telecoms; Bloomberg; The Independent
    - *Should the EU take a unified approach towards Huawei for national security reasons?*

- **Threats to the DNS system highlight the need to protect the Internet's public core**
    - The Russian government acknowledged plans to set up an alternative DNS root server in order to enhance government control over the internet. BBC; IEEE; TechCrunch (2)
    - China's efforts at developing its Great Firewall raise prospects of the export of digital totalitarianism. CSIS; Financial Times; MIT Technology Review
    - The *EU Cybersecurity Act* and the *Paris Call for Trust and Security in Cyberspace* push for the protection of the critical internet infrastructure (albeit without the US, China and Russia). European Parliament; Paris Call for Trust and Security in Cyberspace
    - *What role can the EU play in incentivizing major actors such as China, Russia and the US to join the Paris Call and contribute to the protection of the public core of the Internet?*

- **States are increasingly relying on forward-leaning response mechanisms to counter malign cyber activity from other states**
    - Persistent engagement strategies can expand states' cyber diplomacy toolkits, thus empowering them to deter malicious cyber activities. Lawfare (1); Lawfare (2); Project Syndicate
    - In contrast to the past, states attribute bad behavior more often and supplement diplomatic measures with offensive cyber activities to deter malign actors. EPC; Clingendael
    - *Will the rise in forward-leaning responses to malicious cyber activities reduce the barriers to escalation of conflicts in cyberspace?*

- **Stagnation at the multilateral level has prompted state and non-state actors to develop their own interpretation of norms in cyberspace**
    - The UN First Committee is split between two dueling processes – the Open Ended Working Group led by Russia, and the Group of Governmental Experts led by the United States – constraining big-tent progress. CFR; GPD; Lawfare (3)
    - States have started to publicly expound their national interpretations of how International Law applies to cyberspace in an effort to chip away at the legal grey zones. Just Security; Militair Rechtelijk Tijdschrift; Lawfare (4); Lawfare (5)
    - Industry and civil society are taking a more assertive role in international cybersecurity debates. Tech Accord; Charter of Trust; Fortune; Carnegie; Paris Call; GCSC
    - *How can the Netherlands act at the UN level to mediate tensions between diverging interpretations of international law in cyberspace and convince the G77 countries of a multi-stakeholder approach?*

Conflict in Cyberspace

Global Security Pulse, Strategic Monitor 2019–2020

The Hague Centre for Strategic Studies

Clingendael — Netherlands Institute of International Relations

Long-Term Trends: Development of the International Order

Multi-year Regime Analysis (10-year timespan)

Norms (Acceptance)*	Trend	Rules	Trend
The general integrity and availability of the public core of the Internet should be protected	▲	The degree to which state and non-state actors are adopting measures to protect the Public Core of the Internet (*Paris Call, GCSC, EU Cyber Security Act*).	▲
Electoral infrastructure should be protected	▲	The degree to which state and non-state actors are adopting protective measures to advance article 2(4) of the UN Charter, which articulates this norm and elevates it as a principle of legal, and thus, binding character (*GCSC, United Nations Charter, Paris Call*).	▲
Non-state actors should not engage in offensive cyber operations	▬	The degree to which states are adopting national regulation that prohibits private sector hack-backs (*Paris Call, GCSC Singapore Norm Package, US Active Cyber Defense Certainty Act*).	▼
State critical infrastructure should be protected	▲	The degree to which state and non-state actors are adopting measures to protect their critical infrastructure (*European Parliament NIS Directive, United Nations, UN GGE*).	▲

▲ Increase
▬ Stable
▼ Decrease

■ Increase threat
■ Decrease threat

* Norms are voluntary, legally non-binding commitments, that reflect a common standard of acceptable and proscribed behavior, accompanying and expanding on existing legal understanding rather than attempting to craft new law. It is too early to identify long term trends for norm adherence in the field of international security in cyberspace as the norm-setting process in this space is relatively new – 11 norms were introduced by the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (GGE) in 2013 and 2015. This pulse therefore depicts norm adoption, the degree to which political norms are embedded in (inter)national policies and regulation, and their impact on the international order.