ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON THE CYBER DOMAIN

Issue 9/24 (September)

Bytes and Battles: Navigating Norms in Cyberspace

INTRODUCTION

1. With the increase in players in the cyberspace, rules and regulations are crucial to manage the surge in interactions and potential conflicts. Currently, there are non-binding norms on responsible state behaviour and international laws applicable to maintaining peace, security and stability in cyberspace. However, the unebbing tide of malicious cyber activities, such as espionage, cyber-attacks, misinformation and disinformation, underscores the urgent need for countries to cooperate to ensure that actions in cyberspace are predictable, transparent, and accountable.

THE LEGAL DIMENSIONS – A NEW QUANDARY IN CYBERSPACE CONDUCT

2. Cyber threats are now ranked as the fourth most significant global risk, as highlighted by the World Economic Forum Global Risks Report 2024. The number of cyberattacks has increased globally by 30% in Q2 2024 compared to Q2 2023, and by 25% compared to Q1 2024. The increase in cyber incidents — ranging from cyber espionage to attacks on critical infrastructure and the manipulation of information — pose significant threats to global security and stability.

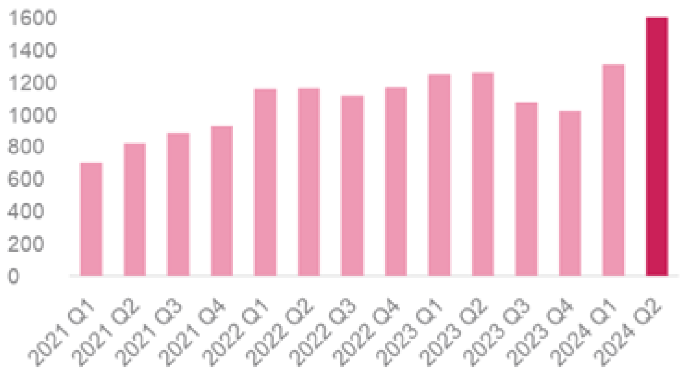

Fig. 1: Average Weekly Cyberattacks per Organisations
(Source: Check Point Research)

3. Cyber incidents can undermine societal values, compromise individual dignity, and exacerbate geopolitical tensions. The 2016 US Presidential Election is a key example of growing concerns about state-sponsored cyber espionage, where state-sponsored operatives allegedly disrupted the process by hacking, releasing sensitive information, and launching disinformation campaigns that increased mistrust. Hence, it is crucial that both state and non-state actors adhere and be accountable to international laws for a safer and more secure cyberspace.

GLOBAL DISCUSSIONS AND INITIATIVES ON CYBER NORMS

4. At the moment, international frameworks and initiatives on responsible behaviour in cyberspace play a crucial role in maintaining global security and stability. Key international frameworks, such as those developed by the United Nations (UN) and the North Atlantic Treaty Organisation (NATO), have laid the groundwork for establishing these norms.

a. The UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE). The GGE has been instrumental in defining norms for state behaviour, including the principle of non-interference in the internal affairs of other states and the protection of critical infrastructure from cyberattacks. In 2015, the GGE consolidated a framework that implemented the 11 norms of responsible state behaviour in the cyberspace which was subsequently endorsed by consensus by all States at the UN General Assembly in 2015. In the 3rd Annual Progress Report adopted by consensus in Jul 2024, States agreed to include a “Norms Implementation Checklist”, and agreed to have further discussions to develop it further.

These norms serve as a baseline for responsible state conduct in cyberspace, promoting a secure and stable digital environment.

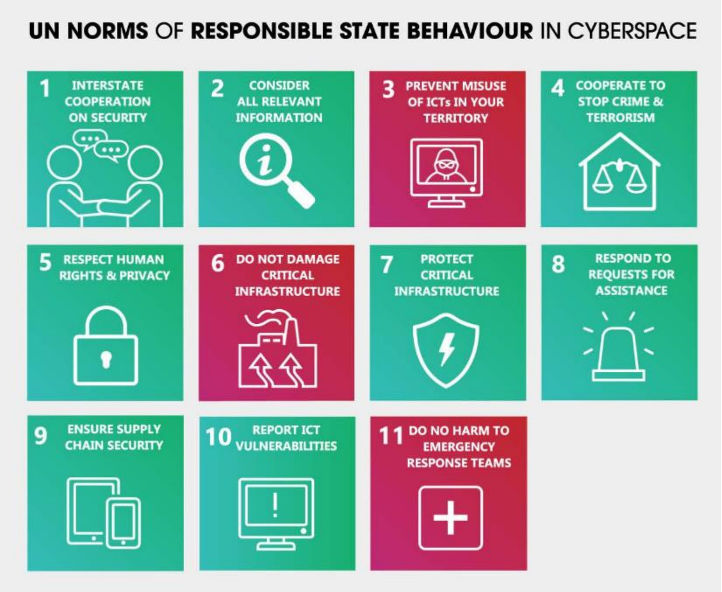
UN NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE
1 INTERSTATE COOPERATION ON SECURITY
2 CONSIDER ALL RELEVANT INFORMATION
3 PREVENT MISUSE OF ICTs IN YOUR TERRITORY
4 COOPERATE TO STOP CRIME & TERRORISM
5 RESPECT HUMAN RIGHTS & PRIVACY
6 DO NOT DAMAGE CRITICAL INFRASTRUCTURE
7 PROTECT CRITICAL INFRASTRUCTURE
8 RESPOND TO REQUESTS FOR ASSISTANCE
9 ENSURE SUPPLY CHAIN SECURITY
10 REPORT ICT VULNERABILITIES
11 DO NO HARM TO EMERGENCY RESPONSE TEAMS

Fig. 2: UN Norms of Responsible State Behaviour in Cyberspace (Source: UN GGE)

b. <u>The UN Open-ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security</u>. Commonly referred to as the UN OEWG on Cybersecurity, it was established in 2018 to complement the work of the GGE by providing a more inclusive forum for all UN member states to discuss and develop norms for responsible state behaviour in cyberspace. In the 2021-2025 cycle, the focus has been on norms implementation. The OEWG together with the GGE provides a platform for States share their views on how international law applies to cyberspace and to also be plugged into international discussions on capacity building and confidence building measures.

c. <u>Tallinn Manual 2.0</u>. Another important initiative is the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. The manual, published in 2017 by a group of international legal experts under NATO’s Cyber Defence Centre of Excellence (CDDCOE), is a non-binding academic study that explored how existing international law applies to cyber operations. Although not legally binding, the Tallinn Manual 2.0 serves as a reference for states and policymakers of an interpretation of how existing legal norms can be applied in the evolving domain of cyberspace.

5. Separately, some countries are also leading global efforts to protect civilians and prohibit cyber operations targeting critical infrastructure, with initiatives like the Paris Call for Trust and Security in Cyberspace. A balanced approach that prioritises the well-being of individuals and the stability of societies builds confidence among states, reducing the likelihood of cyber-related conflicts and fostering a collaborative approach to addressing common challenges in the digital domain.

6. By adhering to internationally agreed norms, states can mitigate these risks and promote a more secure and predictable cyberspace environment. National cyberspace policies can also contribute to societal stability, as they foster an environment where trust is established and maintained between governments, and between states and their citizens. To date, over 70 countries have adopted such national cybersecurity strategies. This trust is fundamental to the effective functioning of the global digital ecosystem, as it reduces the likelihood of conflicts and enhances cooperation on transnational cyber issues.

ASEAN EFFORTS AND CYBER DIPLOMACY

7. In 2018, ASEAN leaders expressed a commitment to operationalise the 11 UN norms of responsible state behaviour in cyberspace as a core element in ASEAN's approach to promoting regional stability in cyberspace. That same year, the ASEAN ministers responsible for cybersecurity subscribed in principle to the norms. At the 2019 ASEAN Ministerial Conference on Cybersecurity, they agreed to establish a working committee to develop a framework for implementation. For ASEAN member states, aligning with these global norms is not only beneficial but necessary to enhance regional cooperation and mitigate the risks of cyber conflicts. Harmonising national laws with these international standards is a critical step toward achieving a unified approach to cybersecurity within the region.

8. Cyber diplomacy has emerged as a vital tool in fostering international cooperation and dialogue on cybersecurity issues. Within the ASEAN region, cyber diplomacy plays a pivotal role in enhancing cooperation, building capacity, and establishing common norms to promote regional stability. ASEAN has been

proactive in advancing regional cybersecurity cooperation through various initiatives. One of the key strategies is encouraging capacity-building programmes, and real-time information sharing among member states. These efforts not only strengthen the region's collective cyber defences but also build trust and collaboration among ASEAN countries, which is essential for effective cyber diplomacy.

a. Several regional initiatives exemplify ASEAN's commitment to cybersecurity. The **ASEAN Cyber Capacity Program (ACCP)** is one such initiative that focuses on building the technical, policy, and strategy-building capabilities of member states through training, technical assistance, and knowledge exchange. ACCP also hosts the Singapore International Cyber Week (SICW) as a platform for regional cybersecurity dialogue. ACCP’s extension, the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) is tasked with conducting research and training in cyber law, and providing Computer Emergency Response Team (CERT)-related technical training. The **ASEAN Regional Computer Emergency Response Team (CERT)** aims to synergise the individual strengths and areas of expertise of the ASEAN national CERTs to bolster the overall effectiveness of regional incident response capabilities.

b. In the defence and military domain, **the ADMM-Plus Experts’ Working Group on Cybersecurity (EWG-CS)** was proposed by the Philippines in 2016 as a platform to facilitate practical collaboration between ASEAN and the eight Plus countries in cybersecurity. The EWG-CS is responsible for discussing initiatives that promote cooperation on cybersecurity and address regional cybersecurity challenges. Since 2016, two cycles of the EWG-CS have been completed, with the third one to be co-chaired by Cambodia and Australia, with support from ACICE.

c. The **ADMM Cybersecurity and Information Centre of Excellence (ACICE)** was set up in 2021 to prioritise capacity building and information sharing between ASEAN defence establishments on cyberattacks, disinformation, and misinformation. ACICE hosts the annual Digital Defence Symposium (DDS) as a platform for defence officials and cyber and information experts for dialogue on developments in the cyber and information domain. Since 2021, ACICE has published more than 100 monthly reports on regional cybersecurity and information threats. ACICE also launched a Malware Information Sharing Platform (MISP) in Feb 2023, and the ACICE Chat (a Telegram channel) in Jul 2024, that provides AMS exclusive, free access to real-time information on cyber malware and other threats to facilitate timely response and mitigation of cyberattacks.

d. Separately, the **ASEAN Cyber Defence Network (ACDN)** was also set up in 2021 to link the cyber defence centres of all ASEAN member states, with the aim of conducting joint exercises and establishing operational partnerships.

9. These initiatives, coupled with ongoing efforts in cyber diplomacy, position ASEAN as a key player in shaping the future of cybersecurity. By continuing to engage in international and regional dialogues, ASEAN can ensure that it remains at the forefront of global efforts to secure responsible state behaviour in cyberspace.

Fig. 3: ASEAN Representatives at the 8th ASEAN Ministerial Conference on Cybersecurity, Oct 2023 (source: ASEAN.org)

CONCLUSION

10. The rapidly evolving landscape of cyberspace demands ongoing dialogue and international cooperation, especially within the ASEAN region. As cyber threats become more complex, ASEAN member states must take an active role in ensuring regional stability and security. Integrating the 11 UN norms into national cybersecurity frameworks will be an important first step to mitigate risks associated with malicious cyber activities and enhance resilience against future threats. At the same time, strengthening regional collaboration through initiatives

such as the establishment of ACICE and various information-sharing protocols will further bolster ASEAN's ability to address emerging cyber challenges effectively. These measures will secure ASEAN's digital landscape and contribute to global cybersecurity efforts.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • • •

REFERENCES

1. Check Point Research Reports Highest Increase of Global Cyber Attacks seen in last two years – a 30% Increase in Q2 2024 Global Cyber Attacks – Check Point
https://blog.checkpoint.com/research/check-point-research-reports-highest-increase-of-global-cyber-attacks-seen-in-last-two-years-a-30-increase-in-q2-2024-global-cyber-attacks/

2. Significant Cyber Incidents – CSIS
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

3. Paris Call
https://pariscall.international/en/

4. National Cybersecurity Strategies Repository - ITU
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

5. The UN norms of responsible state behaviour in cyberspace - ASPI
https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

6. The Tallinn Manual – CCDCOE
https://ccdcoe.org/research/tallinn-manual/

7. Background to UN Discussions on Responsible State Behaviour
https://nationalcybersurvey.cyberpolicyportal.org/background-to-un-discussions-on-responsible-state-behaviour/

8. Factsheet on ASEAN Cyber Capacity Programme – CSA
https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf

9. ASEAN Cybersecurity Cooperation Strategy (2021- 2025)
https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf