Briefing Paper

Committee: DISEC

Topic: The Question of Cyber Warfare and Digital Espionage between Nations

Chair: Lucas Argent

School: Haberdashers' Elstree Schools

Summary

Cyber warfare is the use of technological capabilities by a state or other group to damage or disrupt the infrastructure of another state, often targeting energy grids, financial systems, military networks, government databases and communication system. Distal espionage is covert operations to steal classified information from other states using technological capabilities such as hacking. Differs from cyber warfare as focused on intelligence gathering rather than disruption.

Limited framework exists at present as a result of the relatively recent emergence of such technologies. A United Nations Group of Governmental Experts (GGE) was established in 2004 composed of selected states. It produced reports in 2013, 2015 and 2021. The UN Open-Ended Working Group in ICT Security ran from 2020 to 2025 to help increase capacity building for developing states and increase transparency. There is no legally binding treaty beyond standard rules of war.

Key issues within the discussion involve a lack of clear definitions, the application of existing international law, the issue of attribution in unclear instances, increased targeting of civilian infrastructure and higher risk of escalation.

This Briefing Paper will explore the ways in which DISEC can solve the issue of cyber warfare by analysing past attempts to solve it, key ethical and practical issues as well as potential solutions which could be implemented.

Definition of Key Terms

Cyber Warfare – State-led or state-sponsored operations conducted through digital means to disrupt, degrade, or damage another state's military, governmental, or civilian systems. Disputed: Whether all hostile cyber operations qualify as "warfare" under international law.

Digital Espionage – Covert cyber activities aimed at accessing, stealing, or monitoring sensitive information from another state. Disputed: Often distinguished from cyber warfare due to its non-destructive nature, though the line is blurred.

Cyber Attack – A deliberate action using digital tools to compromise the confidentiality, integrity, or availability of computer systems or data. Disputed: Threshold at which a cyber attack becomes an "armed attack" remains unclear.

Cyber Operations – Broad term covering offensive, defensive, and intelligence-related activities in cyberspace conducted by states.

Information and Communications Technologies (ICTs) – Digital technologies used to store, transmit, or manipulate information, forming the backbone of cyberspace.

Critical Infrastructure – Essential systems such as energy grids, hospitals, water supply, finance, and telecommunications. Disputed: Scope varies between states, especially regarding private-sector systems.

Attribution – The process of identifying the actor responsible for a cyber operation. Disputed: Technical and political challenges make attribution highly contested.

Plausible Deniability – Ability of states to deny responsibility for cyber operations due to attribution difficulties.

International Law in Cyberspace – Application of existing international law, including the UN Charter and IHL, to cyber activities. Disputed: Extent and manner of application remain contested.

UN Charter – Foundational international treaty governing state conduct, including use of force and self-defence. Disputed: How cyber operations fit within Articles 2(4) and 51.

Use of Force – Actions by a state that rise to a level comparable to kinetic military force. Disputed: Whether cyber operations can constitute use of force without physical damage.

Armed Attack – Severe form of use of force that triggers the right to self-defence. Disputed: No agreed cyber threshold.

Sovereignty – Principle that states have authority over their territory and digital infrastructure. Disputed: Whether cyber intrusions violate sovereignty per se.

Non-Intervention – Prohibition on coercive interference in another state's internal affairs. Disputed: Applicability to cyber influence and espionage.

Norms of Responsible State Behaviour – Non-binding expectations guiding how states should act in cyberspace, particularly in peacetime.

Confidence-Building Measures (CBMs) – Mechanisms to reduce mistrust, such as information sharing and communication channels.

Open-Ended Working Group (OEWG) – UN forum open to all states addressing ICT security issues.

Group of Governmental Experts (GGE) – UN-appointed expert group developing consensus reports on cyber norms and law.

Consensus-Based Process – Decision-making model requiring broad agreement, often slowing progress.

Cyber Deterrence – Strategy aimed at discouraging cyber attacks through threat of retaliation or resilience.

Escalation Risk – Danger that cyber operations provoke wider conflict, including kinetic military responses.

Automation in Cyber Operations – Use of software to autonomously detect and respond to threats. Disputed: Risks of unintended escalation.

Cyber Stability – Condition where cyber activities do not undermine international peace and security.

Civilian Harm in Cyberspace – Indirect damage to civilians caused by cyber operations targeting civilian systems.

Dual-Use Infrastructure – Systems used by both civilian and military actors. Disputed: Complicates lawful targeting.

Accountability – Determining responsibility for cyber operations, especially when conducted covertly or through proxies.

Background Information

Existing International Framework

The majority of existing framework stems from agreements made prior to the development of cyber technology. Article 2 (4) of the United Nations Charter prohibits the use of force against the territorial integrity of the state. There has been significant debate as to how far cyber warfare violates this and similar other measures that predate the development of such technologies. Specifically debate over whether cyber operations constitute a ‘use of force’ or an ‘armed attack’.

The United Nations Group of Governmental Experts (GGE) was established in 2004 with a mandate to examine developments in technology as it relates to international relations. It operates on a consensus basis, meaning all members must approve everything enacted which can lead to slow progress. Three notable consensus reports have been released in 2013, 2015 and 2021 which have affirmed that existing international law applies to cyber warfare and developed voluntary norms including but not limited to not attacking response teams and agreements to assist other states. These aren’t legally binding and are entirely voluntary.

The United Nations Open-Ended Working Group on ICT Security (OEWG) had a mandate from 2020 to 2025 to discuss information security. Unlike the GGE was open to all states. Largely focused on capacity and confidence building in developing states. Measures passed were not legally binding. The Tallinn Manal (2013, updated in 2017) was a document produced by legal

experts commissioned by NATO which provides guidance on the dealing with the issue of cyber security. Not legally binding. Rejected by China, Russia and other non-western countries.

Key Ethical Issues

International Humanitarian Law mandates a distinction between civilian and military targets which becomes harder to enforce as a result of the interconnected nature of cyber space. Attacks on power grids can have significant negative impact on civilian populations beyond intended military targets. Cyber warfare has often been used to targets Hospitals and financial systems causing civilian harm.

Proportionally in retaliation becomes harder to assess. Extent of harm and extent of intended harm are difficult to measure through cyber warfare. In addition to being unethical this also heightens the risk of escalation as certain actors may over retaliate in the face of ambiguity leading to further risk of conflict. This is furthered due to the low cost and low risk of immediate casualties in cyber conflict the threshold for conflict is reduced.

The question of attribution and responsibility limits enforceability of accountability mechanisms. Cyber operations are hard to track, made harder by the use of proxy groups and other masking technologies. This makes reliably finding culprits much harder. Even if individual nations are identified, it can be hard to prosecute individuals involved due to a lack of direct harm caused and an inability to discover individuals who carry out attacks within states or organisations.

Technological Overview

There have been rapid advances in the development of software systems for use for cyber security purposes. This had led to increasing integration into military systems, including but not limited to malware attacks, distributed denial of service attacks and supply chain attacks.

Such technologies have had incredibly rapid expansions both in civilian use and military integration. This has made regulation harder as there are constant advancements and changes making regulation and information quickly become redundant. Furthermore, the potential implications on civilian technological development must also be considered.

Cyber Warfare operates within computing frameworks, relying on internet networks, undersea data cables and other software. Cyber capabilities are software based, easily replicable and low cost allowing for easy utilisation.

Major Countries and Organizations Involved

Countries that have been pushing for clearer rules and stronger restraints in cyberspace have included countries from the global south and many European countries. Countries such as Brazil (often speaking on behalf of large cross-regional groups), India, South Africa, Mexico, and numerous African and Latin American states argue that the current situation favours technologically advanced powers. They have supported clearer norms, stronger political

commitments, and movement toward binding rules that would protect critical civilian infrastructure and limit destabilising cyber operations. Their concerns consistently focus on vulnerability, primarily systems such as hospitals, power grids, financial systems, and government services. In less cyber-capable states these are often poorly defended leaving them vulnerable.

European states such as Germany, France, the Netherlands, and Switzerland have generally supported these proposals, though often with more emphasis on legal clarity. They have generally agreed that current international regulations should be applied in the cyber space. Equally, they have called for the introduction of binding regulation to be implemented.

The UN Secretary-General has warned that unchecked cyber operations could undermine international peace and security. His office has consistently called for restraint, stronger international agreements over accepted practise, and better mechanisms for cooperation and transparency.

Major cyber powers, including the United States, Russia, and China have opposed restrictive measures. The United States has argued that existing international law frameworks are sufficient and that harsh regulations could limit technological advancement. Russia and China also emphasise sovereignty and non-interference, though they often interpret these principles differently from Western states. Both have supported discussions on norms but remain cautious about transparency or rules that could expose intelligence activities. This approach has been supported by other states including the UK and Australia.

Cybersecurity firms, academic experts, and think tanks have impacted discussion so far. Civil society organisations and digital rights groups, such as Access Now and the Electronic Frontier Foundation, push attention toward civilian harm, human rights, and the impact of cyber espionage on privacy and freedom of expression.

Timeline of Events (Relevant UN Treaties)

1945 – Article 2(4) of the United Nations Charter. Prohibits the use of force against the territorial integrity against independent states. Drafted prior to the rise of cyber warfare but currently the primary legal basis for assessing the actions of states.

1998 – UN General Assembly Resolution 53/70. First Formal UN resolution addressing the problem of digital information in the context of security. Initiated discussion over cyber threats and security risks.

2001 – Budapest Convention on Cybercrime. This was the first binding international treaty addressing cyber offences. Established framework for investigating cybercrime through international collaboration. However, focuses mainly on individual criminal not states. Russia and China are not parties to the convention.

2004 – Establishment of the GGE. As discussed above, expert body with a mandate to discuss international information security and how international law applies to the cyber space. Not legally binding.

2020 – Establishment of the OEWG. Created to increase capacity within developing states and build confidence in dealing with societal threats. Discussed in more detail above.

2021 – Adoption of both GGE and OEWG reports. Consensus reports were successfully adopted in both bodies confirming the applicability of existing international law applied in the cyber space, including state sovereignty and the right to self defence.

Previous Attempts to Solve the Issue

UN attempts through the GGE to reach consensus agreements have proved largely ineffective. Although reports and agreements have been reached, progress has been slow as a result of the consensus decision making process of the GGE. The outcomes of reports published aren't binding. This has seen the continued utilisation of such tactics in warfare. However, the group has been successful in reaffirming the importance of pre-existing international law.

Confidence and capacity measures in developing nations have also been utilised. These have been promoted both through UN groups such as the OEWG and regional authorities with the aim to increase dialogue between states, limit the harms of cyber attacks and prevent escalation. These have proved moderately successful. However, they have been limited as a result of their voluntary nature and often high associated cost. Equally fails to address offensive capabilities.

Indirect approaches by broader regulation of civilian cyber crime have also been implemented, most notably through the Budapest Convention on Cybercrime. Internationally binding agreement allowing for cooperation increasing dialogue and easier prosecutions. Focused primarily on criminal hacking, fraud and date interference. Ultimately, largely ineffective for solving specifically the issue of cyber crime as it wasn't targeted for this purpose. It also failed to gain unilateral support, with neither China or Russia being parties to the convention.

Possible Solutions

1. Legally binding treaty addressing the issue. Would prove effective as legally binding, allows for clear definitions and effective updated protocols in response to issues. Could involve inclusion of verification and reporting mechanisms, mandating global cooperation and assistance. However, unlikely to be supported by cyber powers such as the USA, Russia and China who are needed, and would have to be done outside of the UNGA or DISEC, due to the inability of UN committees outside of the UNSC to pass binding resolutions. Equally, may quickly become outdated as technology continues to develop.
2. Soft law approach through political declaration. Encourage individual states to regulate, reinforce humanitarian principles and declare opposition to cyber warfare. This approach

does not require support from opposed powers but equally isn't legally binding and so cannot ensure compliance.

3. General regulation on the development of cyber warfare technologies. More direct regulation over dual use technology and technology for civilian purposes will slow down the rapid development of these systems. This will reduce the prevalence of such short term and allow international law to keep up with regulations.
4. Continuation of norm building to create a new international framework. Relies upon existing institutions making implementation relatively easier. However, not politically binding and progress likely to be slow as a result of the need for consensus decisions.
5. Capacity and confidence building in developing states to allow for better resistance and knowledge to respond to cyber attacks. Prevents less developed states from being disadvantaged. Doesn't rely on support from established cyber powers. However does nothing to limit the constant expansion of offensive cyber capacities.

Bibliography

1. UN Office for Disarmament Affairs – Cybersecurity
   https://www.un.org/disarmament/ict-security/
   Central UN hub for information on cyber security, norms, GGEs, and OEWGs.
2. Open-Ended Working Group (OEWG) on ICTs (2021–2025)
   https://www.un.org/disarmament/open-ended-working-group/
   Official documents, reports, and meeting summaries from the inclusive UN cyber process.
3. UN Group of Governmental Experts (GGE) on ICTs
   https://www.un.org/disarmament/group-of-governmental-experts/
   Background and reports from the expert-based UN cyber negotiations.
4. UN Secretary-General's Reports on ICTs and International Security
   https://www.un.org/disarmament/sg-reports/
   High-level assessments of cyber threats, norms, and global risks.
5. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (NATO CCDCOE)
   https://ccdcoe.org/research/tallinn-manual/
   Authoritative academic analysis of how international law applies to cyber warfare.
6. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)
   https://ccdcoe.org/
   Research, legal analysis, and policy work on cyber conflict and defence.
7. International Committee of the Red Cross – Cyber Operations and IHL
   https://www.icrc.org/en/war-and-law/weapons/cyber-warfare
   Humanitarian perspective on cyber operations and civilian protection.
8. Council on Foreign Relations – Cyber Operations and State Conflict
   https://www.cfr.org/cybersecurity
   Accessible analysis of major cyber incidents and state behaviour.

9. Carnegie Endowment – Cyber Policy Initiative
   https://carnegieendowment.org/cyber
   In-depth research on cyber norms, deterrence, and international stability.
10. Chatham House – International Security & Cyberspace
    https://www.chathamhouse.org/topics/cyber-security
    Policy-focused analysis on cyber conflict and governance.
11. European Union – Cyber Diplomacy Toolbox
    https://www.consilium.europa.eu/en/policies/cyber-diplomacy/
    Example of regional approaches to responding to malicious cyber activity.
12. Microsoft Digital Defense Report
    https://www.microsoft.com/security/business/security-intelligence-report
    Private-sector insights into state-sponsored cyber operations.
13. Google Threat Analysis Group (TAG)
    https://blog.google/threat-analysis-group/
    Reports on cyber espionage and influence operations linked to states.
14. Access Now – Human Rights in Cyberspace
    https://www.accessnow.org/cybersecurity/
    Civil society perspective on cyber operations and human rights impacts.