

Committee: DISEC 2

Topic: The Question of State-Sponsored Cyber Crime

Committee Chair: Uliana Tokolova

School: Royal Russell School

Summary

State-sponsored cyber-crime is a growing and complex threat in the modern digital age. It involves cyber-attacks and criminal activity directed or supported by nation-states, often for strategic, military, economic, or political advantage. These operations range from espionage and theft of intellectual property to disruptive attacks on critical infrastructure. Unlike traditional cyber crime, state backed operations often have virtually unlimited resources, highly trained teams, and protection from prosecution in their home country. Major incidents such as the SolarWinds breach, Chinese-linked espionage on U.S. government email systems, and Russian cyber operations in Ukraine show the global reach and severity of these attacks. Attribution is a persistent challenge: even when strong evidence points to a state actor, proving responsibility to an international standard is difficult. The United Nations and other bodies have begun to establish norms for responsible state behaviour in cyberspace, but enforceable rules are still lacking.

Definition of Key Terms

State-Sponsored Cyber Crime – Malicious cyber activities undertaken by, or with the backing of, a government. These operations may target other states' institutions, private companies, or individuals to advance national interests.

Advanced Persistent Threat (APT) – A prolonged, targeted cyber-attack conducted by skilled adversaries, often associated with state actors, which maintains persistent access to a system to extract data or cause disruption.

Attribution – The process of identifying the perpetrator of a cyber-attack. It requires technical evidence, intelligence gathering, and political consensus, and is complicated by anonymisation techniques.

Critical Infrastructure – Systems vital to national security and daily life, including energy grids, transport networks, water supplies, healthcare systems, and communications networks.

Cyber Espionage – The covert use of cyber tools to access and steal sensitive or classified information from governments or private entities.

Background Information

Since the early 2000s, the internet has evolved into a battlefield where states compete for intelligence, influence, and strategic advantage. State-sponsored cyber operations are not new, but their scale, sophistication, and ambition have increased dramatically. Unlike hacktivists or criminal gangs, state-backed operations are often aimed at geopolitical goals—weakening an adversary’s defences, stealing valuable trade secrets, or influencing public opinion.

The SolarWinds attack (2020) demonstrated the reach of state-sponsored actors. Attackers compromised a widely used software update mechanism, affecting thousands of organisations worldwide, including U.S. federal agencies. Evidence pointed to a Russian state-linked APT group known as “Cozy Bear.”

In 2015, Ukraine’s power grid was disrupted in what experts attribute to Russian state-sponsored hackers. This marked the first confirmed cyber-attack to cause large-scale power outages.

Chinese state-linked groups have been accused of conducting extensive cyber espionage campaigns targeting government, defence, and technology sectors worldwide. In 2023, a Chinese APT reportedly accessed 60,000 U.S. State Department emails, compromising sensitive diplomatic information.

North Korea’s “Lazarus Group” has used cyber-attacks for direct financial gain hacking cryptocurrency exchanges and international banks to fund state objectives in defiance of sanctions.

Iranian-backed cyber actors have been implicated in attacks on Middle Eastern energy facilities and Western critical infrastructure, using ransomware and destructive malware.

Unlike conventional warfare, cyber operations offer plausible deniability, can be conducted remotely, and often avoid immediate, visible retaliation. This makes them an attractive tool for states seeking to achieve strategic objectives without crossing traditional military thresholds.

Major Countries and Organisations Involved

United States of America

Both a frequent target and a major cyber power. The U.S. has accused China, Russia, Iran, and North Korea of cyber espionage and disruptive attacks, and has imposed sanctions in response. Maintains advanced cyber defence and offensive capabilities under U.S. Cyber Command.

Russian Federation

Linked to numerous APT groups, including Cozy Bear and Sandworm, responsible for attacks on foreign elections, energy systems, and government networks. Denies official involvement in these activities.

People's Republic of China

Accused of extensive cyber espionage campaigns targeting intellectual property, government communications, and strategic industries. Allegedly sponsors groups such as APT41 and Hafnium.

Democratic People's Republic of Korea (North Korea)

Uses cyber-crime for financial gain and strategic disruption, including the 2014 Sony Pictures hack and large-scale cryptocurrency thefts.

Islamic Republic of Iran

Backs cyber units accused of attacking financial institutions, government systems, and infrastructure in rival states, often using destructive malware.

European Union (EU)

Coordinates cyber defence through the European Union Agency for Cybersecurity (ENISA) and imposes sanctions on individuals or groups linked to cyber-attacks.

United Nations

Through the UN Group of Governmental Experts (GGE) and Open-Ended Working Group (OEWG), promotes voluntary norms for responsible state behaviour in cyberspace.

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Based in Estonia, CCDCOE conducts research, training, and exercises to strengthen collective cyber defence among NATO and partner nations.

Timeline of Events

Date	Description
2007	Cyber-attacks on Estonia disrupt government and banking services; widely attributed to Russian state-linked actors.
2010	Stuxnet worm targets Iranian nuclear facilities; attributed to U.S. and Israeli cooperation.
2014	North Korean hack on Sony Pictures over film <i>The Interview</i> .
2015	Russian-linked hackers disrupt Ukraine's power grid.
2017	WannaCry ransomware, attributed to North Korea, infects hundreds of thousands of computers worldwide.
2020	SolarWinds supply-chain attack infiltrates U.S. government and corporate networks; attributed to Russian SVR.
2021	Microsoft Exchange Server breach attributed to Chinese state-backed group Hafnium.
2022	Russian cyber-attacks accompany invasion of Ukraine, targeting government and media sites.
2023	Chinese-linked hackers breach U.S. State Department emails.

Relevant UN Treaties and Events

UN Group of Governmental Experts (GGE) Reports

In 2013, 2015, and 2021, the UN GGE published landmark reports outlining voluntary norms for responsible state behaviour in cyberspace. These included commitments to avoid targeting critical infrastructure during peacetime and to improve international cooperation on incident response.

Open-Ended Working Group (OEWG) on ICT Security

Established in 2019, the OEWG continues to meet annually to discuss cyber norms, confidence-building measures, and capacity-building. It is the first UN forum open to all member states on the issue of information and communications technology (ICT) security.

Budapest Convention on Cybercrime

Adopted in 2001 by the Council of Europe (and open to non-European states), this was the first international treaty seeking to address cybercrime by harmonising laws, improving investigative techniques, and enhancing cross-border cooperation.

Tallinn Manual on the International Law Applicable to Cyber Warfare

First published in 2013, with an updated version in 2017, this NATO CCDCOE-led academic study examines how existing international law applies to cyber operations, influencing global debates within and outside the UN.

UN General Assembly Resolution 70/237

Passed in 2015, this resolution endorsed the 2015 GGE consensus report and called for member states to implement the recommended cyber norms, helping to bring these voluntary guidelines into broader international recognition.

Previous Attempts to Solve the Issue

Adoption of the Budapest Convention on Cybercrime - 2001

In 2001, the Council of Europe adopted the Budapest Convention, the first binding international treaty on cybercrime. Although not specifically aimed at state-sponsored activity, it established a

legal and cooperative framework for tackling cyber offences across borders. The United States, Japan, Australia, and many European states signed and ratified the treaty, committing to align their national laws and collaborate in investigations. Russia and China opposed the treaty, arguing it infringed on state sovereignty, and instead pursued their own bilateral and regional agreements.

UN GGE Norm-Setting and Consensus Reports – 2013 to 2015

Between 2013 and 2015, the UN Group of Governmental Experts (GGE) achieved rare consensus on voluntary norms for responsible state behaviour in cyberspace. The 2015 report, endorsed by the UN General Assembly, called on states to refrain from targeting critical infrastructure in peacetime and to cooperate on attribution and investigation of cyber incidents. The U.S., UK, and EU strongly supported these norms; Russia and China agreed in principle but emphasised their own concepts of “information security” that include content control.

U.S. and Allies Attribute WannaCry to North Korea - 2017

In May 2017, the WannaCry ransomware attack infected more than 300,000 computers across 150 countries, disrupting hospitals, transport networks, and businesses. In December 2017, the United States publicly attributed the attack to North Korea’s Lazarus Group, with the UK, Australia, Canada, Japan, and New Zealand joining in condemnation. This coordinated attribution marked a rare, unified public stance against a state-sponsored cyber-attack.

Coordinated Sanctions Against Russian Cyber Units - 2020

Following the SolarWinds supply-chain attack, attributed to Russia’s SVR intelligence agency, the United States imposed sanctions in April 2021 on Russian government agencies and technology firms involved. The EU and UK also introduced asset freezes and travel bans on individuals linked to the operation. These measures aimed to deter further state-sponsored hacking by raising the political and economic cost.

Joint Cybersecurity Advisories on Russian and Iranian Threats - 2022

In 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the UK’s National Cyber Security Centre (NCSC), Australia’s Cyber Security Centre, and Canada’s Centre for Cyber Security issued joint advisories warning of increased activity by Russian and Iranian

state-linked hackers targeting critical infrastructure. These advisories included technical details, mitigation guidance, and intelligence-sharing channels, enabling governments and private companies to bolster defences.

Possible Solutions

Cyber Confidence-Building Measures

Encourage transparency through advance notifications of large-scale cyber exercises, establishment of crisis hotlines, and joint incident investigations.

Binding International Treaty

Negotiate a UN-backed treaty prohibiting certain cyber operations (e.g., against critical infrastructure) with enforcement and verification mechanisms.

Global Attribution Mechanism

Establish an independent, internationally recognised body to investigate and publicly attribute major cyber incidents to hold states accountable.

Bibliography

<https://www.phoenixs.co.uk/resources/blog/what-is-a-state-sponsored-cyber-attack/>

https://yjolt.org/sites/default/files/20_yale_j._l._tech._376.pdf

<https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>

<https://onlinelibrary.wiley.com/doi/10.1111/1745-9133.12646>

<https://researchbriefings.files.parliament.uk/documents/CBP-9821/CBP-9821.pdf>

<https://ccdcoe.org/uploads/2018/10/Shackelford-State-Responsibility-for-Cyber-Attacks-Competing-Standards-for-a-Growing-Problem.pdf>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>

<https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level>