ODUMUNC 2021 Issue Brief
GA First Committee (DISC)

# Cyber Security: Cyber Crime, Attacks and Terrorism

*Nick Myers*
ODU Model United Nations Society

## Introduction

Technology has revolutionized the interconnectedness of the globe. The flagship of that globalization is the Internet. However, like all other interconnecting technologies before it, the Internet can become a weapon in the eyes of states, criminals, and terrorists alike. Known as either cyber war or cyber conflict, these attempts to disrupt information technology systems have provoked an increasingly desperate debate on how to respond.


As UN Member States struggle to protect their networks and linked infrastructure from disruption, security against foreign-based attacks has become vital. Member States are concerned about the potential to affect individuals, corporations, states, and regional systems. The anonymity of attacks is a major part of the problem; attackers can swiftly disable individuals, government agencies and private firms, without revealing who carried out the attack in the first place.

Given the transnational nature of many of these attacks, international organizations like the UN have been increasingly pressured to address the rise of cyber-attacks and the security measures against them in the hope of eliciting new international regulations regarding cyber security. Yet, the UN is not without problems of its own in addressing the issues surrounding cyber security and cyber terrorism.

Broadly, the UN is faced with a major roadblock related to cyber. Member States have varied positions on whether the UN should have oversight over what a nation does in cyberspace. Some Member States insist current international laws can sufficiently deal with cyber threats. Other Member States fear expanding international law will be used to narrow their national power, or might undermine their freedom of action.

Currently, cyberspace is viewed as an extension of international law, meaning cyber-attacks are viewed as legally the same as physical attacks rather than as separate issue without its own norms. There is some interest within the General Assembly and the Security Council to address cyber threats by creating new norms for cyber response and use. But the disconnect between the international dangers and national capabilities in cyberspace weakens the potential for forceful UN action, even when it is needed most.

Many Member States want the entire UN community to take an active role responding to the threats posed by cyber-attacks. They say that more effort needs to be put into this issue within the General Assembly especially, since that is where global moral principles are agreed. The current ambiguity surrounding cyber-attacks leaves long standing questions about the definition and meaning of an attack and its consequences in doubt. The ambiguity

undoubtedly helps attackers and those who would use the Internet for malicious purposes.

Growing demands for new rules and approaches to cyberspace have been heard from several Member States. This shift led to several resolutions over the past few years. But other Member States worry that international action could be a veil for efforts to restrict their freedom of action, or advance the particular interests of specific countries. Where growing demands for action will lead is hard to judge.

In an ever-integrating global economy, the prospect of cyber threats looms over everyone. The U.N. remains the most prominent forum for addressing global issues. Important steps have been taken to address these threats, including in the General Assembly, Security Council, and several UN technical organizations. These have established important principles to guide international action. But calls for more aggressive action have gone unmet. If Member States wish for a true universal approach to solving the issues of cyberspace, more work needs to be done.

## History of Cyber Crime

The trajectory of cybercrime in global politics has been on the rise as internet connectivity and other aspects of information technology have spread around the globe. While there is no standing agreement on an international definition of cyber-attack or cyber terrorism within the U.N., rough working definitions have been considered to be broad sweeping online criminal activity in all of its forms. Generally, a cyber crime or attack must serve a destructive or illegal goal. Cyber terror pursues political objectives through cyber actions to harm, coerce, or intimidate a population or state.[1]

Much like terrorist attacks, the perpetrators of cybercrime are difficult to identify unless such attacks are claimed by a specific organization. Many attacks remain unclaimed, no matter which victim is attacked. There have been repeated identifications of the location of the attackers, but the forensic process typically is very slow. While an attack may happen in minutes, identification of an attacker can take months, under the best circumstance. Over time the occurrences of cyber-attacks have diversified and intensified, with an increasing variety of more noticeable attacks being enacted all over the globe.[2]

Still, the major problem with cyber security is the speculative nature of the threats. The range of possible threats is quite broad, both to governments, businesses, and individuals. Some of the most well-known possibilities include:

- Attacks interfering with internet related networks, installations, server parks, major firms.

[1] *Cyberterrorism* Vienna: UN Office on Drugs and Crime, 2019, https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html

[2] *'Significant Cyber Incidents Since 2006*, Washington, D.C.: Center for Strategic and International Studies, September 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/200901_Significant_Cyber_Events_List.pdf

- Attacks on financial industries such as banking and securities trading.
- Attacks denying access to defense ministry computer networks including email and other sensitive systems.
- Energy industries, electricity generation and distribution, including oil refineries and oil and gas pipelines.
- Interference with critical infrastructure such as emergency services, hospitals, energy generation and distribution, or transportation.
- Attacks on government systems by criminal, terrorist, or revolutionary organizations seeking information.
- Violation of commercial and individual privacy

Still, the groups most likely to carry out a cyber-attack are already incredibly powerful states.[3] Countries like China, Russia, and the U.S. are powerhouses in offensive and defensive use of Information and Communication Technologies (ICT), though other states are more than capable of using cyber weapons.

The playing field is opening up though, as organizations have risen to try and combat cyber-attacks from cyber terrorists. These include international organizations like the UN Office of Counter Terrorism (UNOCT), the International Telecommunications Union (ITU), and reports from organizations like the United Nations Institute for Disarmament Research.[4]

Non-governmental organizations have also seen a sharp rise in popularity, with some of the biggest being the Internet Watch Foundation and the Rand Corporation.

In many cases, these nongovernmental organizations are much more successful in dealing with cyber-attacks and security, simply because they are not tied down by an international system such as the U.N and have more capabilities to not only diagnose attacks but also prevent them. The organizations above are a few of the many entities created to combat the ever-growing scope and nature of the cyber realm.

## The Current Situation

The bulk of these cyber-attacks have been largely attributed to a variety of hackers and sparse few terrorist organizations, but there have been prominent attacks by states against other states over the course of the past fourteen years. Below are some prominent examples of attacks designed to disrupt information networks, access critical materials, destroy data, or mislead the public of various states.

- In 2009-2010 the United States and Israel launched a virus, variously known as Stuxnet, Flame or Olympic Games, against Iranian nuclear enrichment centrifuges at its nuclear fuel facility at Natanz, south of Tehran.[5] The Stuxnet attack shut down ten percent of Iran's uranium enrichment capabilities for a full year and set back Iran's nuclear plans even longer. The Stuxnet virus is

[3]James Andrew Lewis, 'Dismissing Cyber Catastrophe', *Center for Strategic and International Studies*, 17 August 2020, https://www.csis.org/analysis/dismissing-cyber-catastrophe

[4] Camino Kavanagh, *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*. Geneva: United Nations Institute for Disarmament Research, 2017, https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf;

[5] David E. Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *New York Times*, 1 June 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

widely thought to have operated by targeting nuclear centrifuges through flash drives, not via the internet. Even after ten years, Stuxnet remains one of the most successful and visible shows of what a cyber attack can accomplish. It has seen wide praise and condemnation within the international community, with some viewing it as a precedent for how cyber will be used in the future, and some seeing it as a blatant abuse of power and intrusion in sovereign affairs.

- Russian involvement in the 2016 US presidential election can also be considered part of a coordinated series of cyber-attacks.[6] This was a broad attack and included thousands of Russian bots on social media sites like Facebook and Twitter meant to spread misinformation and amass support of then-candidate Donald Trump. This included trying to appeal to teens by spreading political memes and patriotic posts. This campaign also included the famous 2016 Democratic National Committee (DNC) hack. Tens of thousands of private emails from top party leaders, including presidential candidate Hillary Clinton, were released to the public via Wikileaks after two online hackers, Fancy and Cozy Bear gained access to the DNC's private servers.[7] These hackers were traced back to Moscow from an independent investigation by the private research group CrowdStrike.

- More examples of cyber-attacks to damage infrastructure happened in Ukraine.[8] Three days before Ukraine's 2014 Presidential election, Russia hacked into the Central Election Commission and disabled part of its network. Since then, there have been several major cyber-attacks on Ukraine, including on a power grid that affected 230,000 people. Russian entities hacked into Ukrainian tech firms to access banks, airports, and government agencies in Ukraine, costing Ukraine upwards of USD 10 billion.

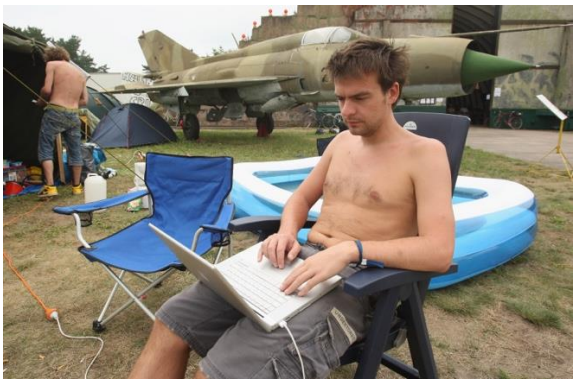
- Australia saw a sharp uptick in attacks from what Prime Minister Scott Morrison called a, 'malicious' and 'sophisticated' state-based actor, starting in June 2020.[9] The attacks were wide ranging, focusing on government, industry, education, health, and critical infrastructure, though no major damage has been made public yet. Australian experts believe China to be the culprit, largely since the attacks came after Australia openly questioned the origin of the coronavirus and whether China was truthful about its reported numbers.

[6] Jonathan Masters, 'Russia, Trump, and the 2016 U.S. Election', *Council on Foreign Relations*, 26 February 2018, https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election

[7] Sam Thielman, ' DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach', *Guardian*, 26 July 2018, https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2

[8] Laurens Cerulus, 'How Ukraine became a test bed for cyberweaponry', *Politico*, 14 February 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

[9] Angus Watson and James Griffiths, ' Australia says it has been targeted by a 'sophisticated' state-based cyber attack', *CNN Business*, 18 June 2020, www.edition.cnn.com/2020/06/18/tech/australia-cyber-attack-intl-hnk/index.html



These attacks and many others demonstrate that cyber-attacks are a far-ranging means of projecting state power to negatively impact another state, community, or group of people potentially on the other side of the globe. The inability of the victim to rapidly identify their attacker makes these attacks much more difficult to defend against.

## Role of the UN

The emerging issue of cyber security has made it a relevant issue to all UN organizations, either because those bodies utilize the internet or because they are responsible for ensuring access and protecting state interests. While the UN has condemned all types of cybercrime and attempted to increase access to defensive technologies, it has also failed to sufficiently address the issue. Rival interests and priorities of Member States make it difficult for the UN to agree on basic principles. The lack of focused attention on cyber security, cyber terrorism, and cyber-attacks has slowed forceful action against cyber terrorism and cybercrime. Part of this is simply because cyberspace is such a large and complicated subject, hard to pack into even a few organizations or resolutions.

A more fundamental weakness comes from the tendency of the international community to view cyber threats as a new branch of existing issues.

For example, the UN couples human trafficking and cyber trafficking as a single trans-national crime issue, treating cybercrime as an extension of other kinds of crime under international law. While appropriate for an organization to attempt to work against broad-reaching criminal organizations, this coupling of other issues to cyber inhibits the development of new norms, resolutions, and agreements tailored to addressing cyber-specific issues on the broad-spectrum of cyber security concerns. Thus, no new, global cyber laws have been created to treat these as unique issues.

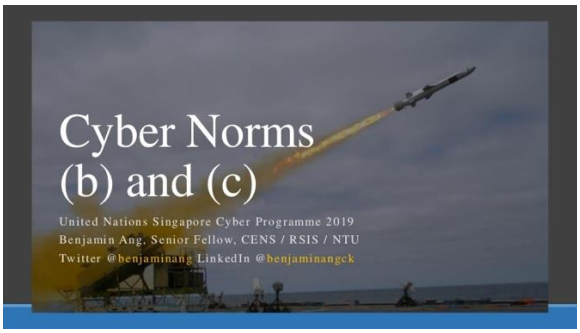
Critics say this leads to a false feeling of adequacy within the organization, a comfort in the familiar capabilities of sub-organizations to address issues like crime or terrorism. Yet, without a unique cyber-specific sub-organization it becomes difficult for the UN to respond to the changing situation surrounding cyber as a whole, thus serving to highlight a disconnect between wanting to act on cyber as a specific Member State and the organization as a whole feeling comfortable with the inadequate status quo despite the increasing frequency of prominent cyber-attacks.

Finally, the existing UN system on cyber threats is paralyzed to address cyber issues once they arise. Frequently, the General Assembly or Security Council will not mention cyber, with it coming up less than 5 times in the last 3 years.[10] Given the volume of cyber-attacks occurring each year coupled with the dynamic nature of cyber, this is remarkably low. If the subject is brought up, there is usually disagreement about how a global effort to combat cyber threats would work, with states such as Russia wanting more universal participation in creating mandates on cyberspace involving all members

[10] *General Assembly Resolutions.* New York: United Nations, 2020, www.un.org/en/sections/documents/general-assembly-resolutions/

through an inclusive Open-Ended Working Group (OEWG), while the US and UK want top ranking members to report on and create mandates for the rest of the world via a Group of Governmental Experts (GGE).[11] There is no denying that the UN and its members want to create a more stream-lined cyber strategy, but endless in-body debates means any universal acceptance of new laws and cyber security remains unlikely if there is not a vast uptick in discussion and relevance of cyber within the UN as there is disagreement regarding how the organization should respond to future developments.

Despite these shortcomings, there remain several entities working on cyber security and assisting the UN. The Geneva-based International Telecommunications Union (ITU), an independent international organization affiliated with the United Nations, has emerged as the center for international coordination on these issues. By setting standards for all telecommunications, it provides essential benchmarks for governments, establishing what is universally accepted as permissible and where limits are for governments. UN General Assembly and ECOSOC relations usually mandate the ITU as the center for further consideration and action. The ITU has set up a global cyber security index (GCI) in an effort to bring more attention to cyber threats worldwide in coordination with the UN.[12] This is meant to keep an up active list of both cyber-attacks and useful strategies to defend against attacks so Member States can better deal with cyber security issues. The ITU also assists in designing cyber security plans and infrastructure for member states.




Other, smaller bodies within working to combat cyber terrorism include the UNOCT's Cybersecurity Programme, which focuses on enhancing state capacity and private organizations in preventing cyber-attacks, and the Office on Drugs and Crime's (UNODC) Global Programme on Cybercrime, which focuses on capacity building and technical assistance of cyber networks and defensive systems. These bodies offer the main source of energy and effort in combatting cyber-attacks and improving security for Member States, but each of these organizations is limited due to lacking the support of a coordinating mechanism to assist each disparate UN organization in addressing cyber security developments together. Thus, the UN is left with several organizations going in different directions rather than a unified approach capable of constructing international norms, regulations, or mandates.

Taken as a whole, this reveals a UN framework that is hardly adequate for a weapon system and problem which is rapidly transforming, becoming more prevalent, and holds the potential to significantly disrupt global relations. Inaction can only take the UN so far, and the cobbled together nature of current UN programs indicates the issue is setting the pace for the

[11] *Group of Governmental Experts*. New York: United Nations Office for Disarmament Affairs, 2019, www.un.org/disarmament/group-of-governmental-experts/

[12] *United Nations Launches Global Cybersecurity Index*. Geneva: International Telecommunication Union, n.d., https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx

organization rather than the organization being proactive in developing a regime for the future.

## Landmark UN Resolutions

Over the past several years there have been attempts to turn the UN to address cyber security and cyber issues uniquely through resolutions within the Security Council and the General Assembly. Unfortunately, very few of these resolutions broke enough ground to be truly transformative for UN policy, but they remain influential in being the most significant efforts within the most significant international bodies to do something regarding cyber issues.

- **Security Council resolution 2341** (passed in 2017), established a process, continuing to this day, to establish 'best practices' to protect critical infrastructure from cyber-attacks in coordination with Interpol, UN Counter-Terrorism Centre, and the Counter-Terrorism Committee Executive Directorate.[13] This help states stay informed about potential cyber risks they need to counter.

- **General Assembly resolution 74/173 (2019)** focused primarily on development of Member States capacity building to respond to cybercrime brought in components of cooperative objectives.[14]

- **General Assembly resolution 74/28 (2019)** presented standards for responsible state behavior in cyberspace for international security purposes.[15] Of greatest importance was establishing international norms, regulations, laws, and non-binding resolutions to cyber technology environments.

- **General Assembly resolution 73/266 (2018)** focused on the development and codification of international principles for cyberspace, with a particular focus on the impacts of it financially.[16]

- **General Assembly resolution 73/187 (2018)** on countering criminal activity, seeks more international cooperation to stop criminal organizations utilizing communications platforms to commit crimes.[17] Importantly it called for improving the technical infrastructure of developing states to address this concern through assistance through the UN.

These resolutions illustrate an attempt to develop a response to challenges related to cyber developments, but fall short of providing a landmark policy trajectory for the UN. Instead, they establish the importance of the issue, the role of the UN on the subject, and the potential dangers for states ignoring the problem.

---

[13] *The protection of critical infrastructure against terrorist attacks: Compendium of good practices*. Vienna: United Nations Counter-Terrorism Centre, 2018, https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf

[14] *Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing*, resolution 74/173. New York: United Nations, 2019, https://undocs.org/en/A/RES/74/173

[15] *Advancing responsible State behaviour in cyberspace in the context of international security*, resolution 74/28. New York: United Nations, 2019, https://undocs.org/en/A/RES/74/28

[16] *Advancing responsible State behaviour in cyberspace in the context of international security*, resolution 73/266. New York: United Nations, 2018, https://undocs.org/en/A/RES/73/266

[17] *Countering the use of information and communications technologies for criminal purposes*, resolution 73/187. New York: United Nations, 2018, https://undocs.org/en/A/RES/73/187

## Country and Bloc Positions

Issues like cyber security attract a host of differing opinions, beliefs, and philosophies concerning the role of international governance, institutions, and the role of the state within cyber space. Broadly, states divide into two camps where the first believes cyberspace should be the purview of states and the second believing there is a critical role for international governance in cyberspace. Interestingly, several states only became concerned over the developments related to cyber because they have experienced significant cyber-attacks recently including **Australia[18], India[19], and Indonesia.** Other critical players on the issue include:

**China:** Famous for the 'Great Firewall' that blocks mostly European and UN tech firms from its internet, China has stressed its sovereign control over all other goals. Second, it seeks to expend influence, through its own firms, and through control over UN agencies. China has readily adopted, utilized, and developed cyber capabilities at an astounding rate.[20] Viewing cyberspace as a new realm for interacting within the international community, China specifically focuses on its own domestic information security to prevent dissent. It favors international cooperation in response to threats while retaining its own state autonomy.

**Democratic Republic of Korea (North Korea):** Although it is not a major force in the UN North Korea could be a target of future UN resolutions. North Korea represents an interesting major player when it comes to cyber security concerns.[21] Favoring asymmetric cyber-attacks geared towards disrupting target operations and provocations to justify domestic considerations, North Korea was considered responsible for the Sony Hack in 2014.[22] Additionally domestic censorship and propaganda are heavily utilized. North Korea is widely believed to use cyber activity to augment state income, overcoming UN sanctions to a degree.

**European Union:** The EU and its 27 Member States have been ardent supporters of user information security. They have repeatedly challenged the dominance of American tech firms, and increasingly question those from China, too.[23] In terms of addressing cyber-attacks and terrorism, the EU has established several regional organizations to address the issue. In a move that anticipates its priorities for the UN, it established the EU Cybersecurity Act in February 2020.[24] The EU is highly sensitive

[18] Hafizah Osman, ' Cyber security a top priority in Australia: Deloitte', *Tech Advisor*, 1 November 2012 https://www.techadvisor.co.uk/feature/security/cyber-security-top-priority-in-australia-deloitte-3408391/

[19] Ashish Rajadhyaksha, *In the Wake of Aadhaar: The Digital Ecosystem of Governance in India*. Bangalore, 2013, https://egov.eletsonline.com/2012/11/government-to-invest-200-mn-in-4-yrs-on-cyber-security-infrastructure/; https://www.dnaindia.com/india/report-india-uk-to-conduct-talks-bi-annually-on-cyber-security-1762061

[20] Lyu Jinghua, ' What Are China's Cyber Capabilities and Intentions?' *Carnegie Endowment for International Peace*, 1 April 2019, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

[21] www.csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf

[22] Andrea Peterson, 'The Sony Pictures hack, explained', *Washington Post*, 18 December 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

[23] *Cybersecurity in Europe: stronger rules and better protection*. Brussels: European Council and the Council of the EU, 31 July 2020, https://www.consilium.europa.eu/en/policies/cybersecurity/

[24] *The EU Cybersecurity Act*. Brussels; European Commission, 28 February 2020, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

to Internet security, and especially insistent that the privacy and rights of private users be protected from spying by governments.

**Iran:** Iran has been both a victim and originator of cyber conflict. In 2009 is was attacked by Israel and the US through their Olympic Games (Stuxnet) campaign to temporarily disable part of its nuclear infrastructure. Iran also has been a willing participant in the development of cyber capabilities to address cyber defense and attacks.[25] The Iranian history of significant cyber-attacks is quite large, with a heavy reliance on attacking critical systems for opposing states.[26] Most recently following the American assassination of General Qassem Soleimani, the threat of Iranian cyberattacks increased.[27] In the UN, Iran favors a state-centered approach to cyber security issues like cyber attack

**Non-Aligned Movement:** For the 120 Member States of UN's largest voting bloc, development aspects outrank other concerns. NAM Member States may be willing to join resolutions to tighten international standards or support action against specific countries, even fellow NAM members like DPR Korea or Iran. In exchange they will insist on generous development assistant, such as financial support for their national broadband networks and cyber law enforcement capabilities. The NAM focuses on the threat that fast-changing information and technologies could be used for purposes that are contradictory with maintaining international law and stability.[28] Many in the NAM have proposed that a legal framework be developed within the UN to combat these rising issues.

**Russia:** Although fiercely denied by its leaders and spokesmen, Russia is widely suspected or major internet and social media attacks on against infrastructure (such as electricity generation), news media and electoral systems in countries like Ukraine, the UK and US.[29] Yet, Russia has also been an ardent supporter of UN actions to curtail cybercrime. A significant resolution was passed through the General Assembly, written by Russia.[30] In this sense, Russia has become increasingly skilled at navigating the processes of the UN to further their approach to cyber governance which has been criticized as "digital authoritarianism." They also helped create the OEWG, being the main state to propose new rules and a more universal recognition of cyber. Russia has recently released a statement on the issue of cyber security in lieu of the Covid-19 pandemic.

**The United States:** American cyber security policy focuses on combatting cyber-attacks by securing America's domestic networks and critical infrastructures, along with expanding American influence and norms internationally.[31]

---

[25] James Andrew Lewis, 'Iran and Cyber Power', *Center for Strategic and International Studies*, 25 June 2019, https://www.csis.org/analysis/iran-and-cyber-power

[26] S*ignificant Cyber Incidents*, op.cit., https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

[27] *National Terrorism Advisory System Bulle*tin, Washington, D.C.: U.S. Department of Homeland Security, 4 January 2020, https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-4-2020

[28] 'Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race.', New York: UN General Assembly, 24 October 2016, www.un.org/press/en/2016/gadis3560.doc.htm

[29] Tim Maurer and Garrett Hinck, 'Russia's Cyber Strategy', Milan: Italian Institute for International Political Studies, 21 December 2018, www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835; www.russiaun.ru/en/news/arria_220520

[30] https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/

[31] President Donald J. Trump, *National Cyber Strategy of the United States of America September 2018.* Washington, D.C.: The White House, 2018, www.whitehouse.gov/wp-

The US believes that international cyber stability and conflict prevention are best advanced by current international law. Recently, the U.S has been increasingly aggressive towards cyber threats, increasingly striking suspected threats preemptively. Part of this includes being more open in declaring the suspected culprits of cyberattacks. Cyber has become a massive part of American defense and foreign policy, with proposals in 2019 made by the Cyberspace Solarium Commission to work more closely with the private sector in sharing information with agencies like the NSA and Cybersecurity and Infrastructure Security Agency (CISA).

## Proposals for Action

The UN response to cyberspace is still in its infancy, thus the only precedence lies in similar issues which could be capable in informing or framing resolutions. The pre-existing resolutions offer a framework to proceed in addressing issues related to cyber security, but be aware of what kind of action the U.N has undertaken, whether it be setting up the Group of Governmental Experts to make reports on the use of cyberspace, or sub-organizations like UNODC, UNOCT, and the ITU. These all focus on improving knowledge and security of Member States and businesses against cyber terrorism and crime. Some potential proposals to consider include:

- **Require Internet service providers—the companies that make the internet work—to monitor and enforce restrictions** on use of the Internet to harm the infrastructure or interests of UN Member States. This could be especially popular in Member States that already restrict private Internet activity. It will be opposed by Member States were personal freedom and privacy are more important.

- **Establish an independent UN agency to monitor Internet activity and report to Member States on Internet use and attacks by their citizens or foreign sources.** This also could be especially popular in Member States that already restrict private Internet activity. It will be opposed by Member States were personal freedom and privacy are more important. Financing and staffing for the new agencies would have to be established.

- **Propose a global definition of cyber terrorism, cyber-attacks, cyber security** as part of an effort to establish a foundation for new international laws, rules, and norms.

- **Provide technical assistance to states** to increase their security capabilities against potential cyber- attacks. Financing and paying for technical assistance could be a problem, but countries interested in expanding their global influence might be willing to subsidize such a resolution, if it favors their firms.

- **Sponsor the development of a U.N. framework organization** to coordinate all cyber security responses and considerations.

- **Encourage Member States** to prepare their own defenses. Such a limited proposal might be most popular with Member States determined to protect

content/uploads/2018/09/National-Cyber-Strategy.pdf; 'Cyber-defence ; and, 'America rethinks its strategy in the Wild West of cyberspace', *The Economist*, 28 May 2020, www.economist.com/united-states/2020/05/28/america-rethinks-its-strategy-in-the-wild-west-of-cyberspace

their national sovereignty and avoid new obligations.

- **Establish rules for sanctioning states responsible** for carrying out, funding, or assisting in cyber-attacks against other states, international organizations, or corporations.
- **Finance the development of offensive cyber capabilities** in order to establish deterrent measures to prevent cyber-attacks.
- **Provide the means for the revival of the typewriter construction industry** and other intranet systems**.** After all states cannot hack what is not connected to the internet.

# Bibliography

Center for Strategic and International Studies. *Significant Cyber Incidents Since 2006*, Washington, D.C.: Center for Strategic and International Studies, September 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/200901_Significant_Cyber_Events_List.pdf

Cerulus, Laurens. 'How Ukraine became a test bed for cyberweaponry', *Politico*, 14 February 2019, https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/

Economist. 'America rethinks its strategy in the Wild West of cyberspace', *The Economist*, 28 May 2020, www.economist.com/united-states/2020/05/28/america-rethinks-its-strategy-in-the-wild-west-of-cyberspace

European Commission. *The EU Cybersecurity Act*. Brussels; European Commission, 28 February 2020, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

European Council. *Cybersecurity in Europe: stronger rules and better protection*. Brussels: European Council and the Council of the EU, 31 July 2020, https://www.consilium.europa.eu/en/policies/cybersecurity/

International Telecommunication Union. *United Nations Launches Global Cybersecurity Index*. Geneva: International Telecommunication Union, n.d., https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx

Kavanagh, Camino. *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*. Geneva: United Nations Institute for Disarmament Research, 2017, https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf;

Lewis, James Andrew. 'Dismissing Cyber Catastrophe', *Center for Strategic and International Studies*, 17 August 2020, https://www.csis.org/analysis/dismissing-cyber-catastrophe

Lewis, James Andrew, 'Iran and Cyber Power', *Center for Strategic and International Studies*, 25 June 2019, https://www.csis.org/analysis/iran-and-cyber-power

Lyu Jinghua, ' What Are China's Cyber Capabilities and Intentions?' *Carnegie Endowment for International Peace*, 1 April 2019, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Masters, Jonathan. 'Russia, Trump, and the 2016 U.S. Election', *Council on Foreign Relations*, 26 February 2018, https://www.cfr.org/backgrounder/russia-trump-and-2016-us-election

Maurer, Tim, and Garrett Hinck, 'Russia's Cyber Strategy', Milan: Italian Institute for International Political Studies, 21 December 2018, www.ispionline.it/en/pubblicazione/russias-cyber-strategy-21835; www.russiaun.ru/en/news/arria_220520

Osman, Hafizah.' Cyber security a top priority in Australia: Deloitte', *Tech Advisor*, 1 November 2012 https://www.techadvisor.co.uk/feature/security/cyber-security-top-priority-in-australia-deloitte-3408391/

Peterson, Andrea. 'The Sony Pictures hack, explained', *Washington Post*, 18 December 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/

Rajadhyaksha, Ashish. *In the Wake of Aadhaar: The Digital Ecosystem of Governance in India*. Bangalore, 2013, https://egov.eletsonline.com/2012/11/government-to-invest-200-mn-in-4-yrs-on-cyber-security-infrastructure/; https://www.dnaindia.com/india/report-india-uk-to-conduct-talks-bi-annually-on-cyber-security-1762061

Sanger, David E. 'Obama Order Sped Up Wave of Cyberattacks Against Iran', *New York Times*, 1 June 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

Thielman, Sam. ' DNC email leak: Russian hackers Cozy Bear and Fancy Bear behind breach', *Guardian*, 26 July 2018, https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2

Trump, President Donald J. *National Cyber Strategy of the United States of America September 2018.* Washington, D.C.: The White House, 2018, www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; 'Cyber-defence

UN Counter-Terrorism Centre . *The protection of critical infrastructure against terrorist attacks: Compendium of good practices*. Vienna: United Nations Counter-Terrorism Centre, 2018, https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf

UN General Assembly. *Advancing responsible State behaviour in cyberspace in the context of international security*, resolution 73/266. New York: United Nations, 2018, https://undocs.org/en/A/RES/73/266

UN General Assembly. *Advancing responsible State behaviour in cyberspace in the context of international security*, resolution 74/28. New York: United Nations, 2019, https://undocs.org/en/A/RES/74/28

UN General Assembly. 'Calling for Norms to Stymie Cyberattacks, First Committee Speakers Say States Must Work Together in Preventing Information Arms Race.', New York: UN General Assembly, 24 October 2016, www.un.org/press/en/2016/gadis3560.doc.htm

UN General Assembly. *Countering the use of information and communications technologies for criminal purposes*, resolution 73/187. New York: United Nations, 2018, https://undocs.org/en/A/RES/73/187

UN General Assembly. *Promoting technical assistance and capacity-building to strengthen national measures and international cooperation to combat cybercrime, including information-sharing*, resolution 74/173. New York: United Nations, 2019, https://undocs.org/en/A/RES/74/173

UN General Assembly. *General Assembly Resolutions.* New York: United Nations, 2020, www.un.org/en/sections/documents/general-assembly-resolutions/

UN Office for Disarmament Affairs. *Group of Governmental Experts*. New York: United Nations Office for Disarmament Affairs, 2019, www.un.org/disarmament/group-of-governmental-experts/

UN Office on Drugs and Crime. *Cyberterrorism* Vienna: UN Office on Drugs and Crime, 2019, https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html

U.S. Department of Homeland Security. *National Terrorism Advisory System Bulle*tin, Washington, D.C.: U.S. Department of Homeland Security, 4 January 2020, https://www.dhs.gov/ntas/advisory/national-terrorism-advisory-system-bulletin-january-4-2020

Watson, Angus, and James Griffiths, ' Australia says it has been targeted by a 'sophisticated' state-based cyber attack', *CNN Business*, 18 June 2020, www.edition.cnn.com/2020/06/18/tech/australia-cyber-attack-intl-hnk/index.html