ODUMUNC 2022 Issue Brief
First Committee: Disarmament and International Security

Advancing Responsible State Behavior in Cyberspace

by Carrie Smith
ODU Model United Nations Society

Introduction

Like many difficult issues of international peace and security, cyber security gets to the heart of the issues that divide the 193 member States of the UN most. What matters most? And how to balance conflicting priorities?

For over 20 years the UN has struggled to balance the priorities of individual access and freedom on-line, against the problems of managing the dangers of misuse by criminal, terrorists, and even other states. The UN has to decide if the basic issue is strengthening the principle of national sovereignty, or is it the unifying power of international law? These are painful questions. But if they were easy, the UN wouldn't have to deal with them.

More than twenty years of work and cooperation have enabled Member States to get better at the danger of terrorist exploitation of the internet. But technology continues to shock. The sudden rise of Islamic State—with a powerful on-line presence—in 2014 came as a shock to many.

The international community still struggles to deal the dangerous of criminal and terrorist exploitation of the internet. To that danger a new one emerged, from Member States themselves. Barely imagined in 1998, in the contemporary world attacks by Member States are becoming a major worry.

The original priorities—cybercrime and terrorism—were hard for the UN, mostly due to basic contradictions of the internet; the seeming impossibility to assuring individual access while controlling criminal and terrorist actors. Everything that made internet use easier for ordinary users also made activity easier for cyber-crime and non-state attacks.

The original priorities—fighting cybercrime and counterterrorism—were hard for the UN, mostly due to basic contradictions of the internet; the seeming impossibility to assuring individual access while controlling criminal and terrorist actors. Everything that made internet use easier for ordinary users also made activity easier for cybercrime and non-state attacks.

But at least back then there was less worry about states using the internet to attack other states. The hope was that encouraging states to accept equal normative standards, principles of the kind the UN excels at, would help everyone manage the possibilities and danger. There was general agreement of the need to coordinate the acts of individual states. And international law also was helpful, since it gave Member States a powerful tool to promote global cooperation among states against a shared threat.

It’s no longer that simple. In 2007-09, attacks by member States were emerging as the greatest danger. While criminals spun their frauds and thefts, and terrorists sued the internet to organized attacks, states used it to paralyze whole national networks and shuts down entire industries.

In 2007 a diplomatic conflict between Estonia and Russia took a new form when Estonia suddenly found banks and parts of government shut down on-line. The attack was presumed to come from Russia, but whether it was the work of the Russian government, nationalist sympathizers, or some combination, was never clearly established. In 2009 computers controlling a portion of Iran’s nuclear infrastructure were destroyed. The attack turned out to be a cooperative effort by Israel and the United States. The precedent of state-sponsored and authorize attacks had been demonstrated. Whether this trend can be reversed is up to the Member States of the UN.

Background

Technology has revolutionized the interconnectedness of the globe. The flagship of that globalization is the Internet. Like all other interconnecting technologies before it, the Internet can become a weapon in the eyes of states, businesses, non-governmental organizations, individuals, criminals, and terrorists alike. Known as either cyber war or cyber conflict, these attempts to disrupt or misuse 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.

According to a prominent report, there have been tens of thousands of successful attacks on government agencies, defense and high-tech companies, or economic crimes with losses of more than a million dollars in 2020 alone. Whether it is called computer security, cyber security, or IT security, the problem today is how to ensure governments, corporations, financial institutions, hospitals and other businesses can collect, process and store confidential information on computers. These computers, need secure networks to transmit this information to other computers. With the ever-growing increase and sophistication of cyber-attacks, constant and ongoing attention is required to protect this sensitive information as well as to protect national interests and security.

The development of information and communication technologies (ICTs) have implications for all three pillars of the United Nations’ work: peace and security, human rights and sustainable development.

ICTs and global connectivity have been a catalyst for human progress and development, transforming societies and economies, and expanding opportunities for cooperation. Negative trends in the digital domain could undermine international security and stability, place strains on economic growth and sustainable development, and hinder the full enjoyment of human rights and fundamental freedoms. These trends include the growing use of ICTs for malicious purposes.

UN Member States have varied positions on whether the UN should have a mandatory role over what a nation does in cyberspace.[1] 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 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 helps attackers and anyone 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 UN 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.

The question, however, isn’t why a person, or group, steals information and it isn’t about what they are going to do with the information they stole. The questions most ask are “How did they do it?” and “What did they get?” In an era where cyber-attacks and digital spying are the top threat to national security and eclipsing terrorism, and where you can tweet @ the American Army, how will the international community handle the responsibility of State Behavior in Cyberspace International Security? More importantly, how will states deal with the application of international law to cyberspace ethically?

What is Cyber Security?

There are two sides to cyber security:

- The protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as the disruption or misdirection of the services they provide.

[1] O'Sullivan, Kate. 2021. ‘UN makes critical progress on cybersecurity’, *Microsoft*, 29 March 2021, https://blogs.microsoft.com/on-the-issues/2021/03/29/un-working-group-cybersecurity-report/

- The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign states, hostile or potentially hostile forces or elements, or areas of actual or potential operations; the activities that result in the product; the organizations engage in such activities.

Although one is much more technical, both definitions convey the same basic idea. The purpose of cyber intelligence is to collect, analyze, and process data in order to make targeted decisions that will benefit the user, whether in business or military practices. The action of also defending your own networks typically falls under the branch of cyber security.

Under the umbrella of cyber security, there is a branch titled cyber-data collection. This is closely related to cyber security, seeing as this is where data is not only collected, but also processed in a repetitive manner daily. In order to prevent cyber-attacks most companies have cyber security teams that will begin with planning and direction to determine what data initial target for cyber-attacks. They then gather the intelligence of the data to understand what will be used against them in an attack. The last step is the dissemination of the intelligence gathered to the rest of the company and plan to better secure the information from cyber-attacks.

When a cyberattack occurs a cyber security team analyze what data was collected from an attack and analyzes it to better assess the threat. Cyber espionage, or cyber spying, is a type of cyberattack in which an unauthorized user attempts to access sensitive or classified data or intellectual property for economic gain, competitive advantage or political goals.

Cyber Espionage

Cyber espionage is a means to gather sensitive or classified data, trade secrets or other forms of Intellectual property that can be used by the aggressor to create a competitive advantage or sold for financial gain. In some cases, the breach is simply intended to cause reputational harm to the victim by exposing private information or questionable business practices. Cyber espionage also can mean hacking and destructive attacks, when sponsored by a state intelligence agency.
Much of cyber espionage is commercial. Attacks can be motivated by hope of monetary gain; they may also be deployed in conjunction with military operations or as an act of cyber terrorism or cyber warfare. The impact of cyber espionage, particularly when it is part of a broader military or political campaign, can lead to disruption of public services and infrastructure, as well as loss of life.

Typical espionage targets include but are not limited to: research and development data and activity, academic research data, Intellectual Property, such as product formulas or blueprints, salaries, bonus structures and other sensitive information regarding organizational finances and expenditures, client or customer lists and payment structures, business goals, strategic plans and marketing tactics, political strategies, affiliations and communications, and military intelligence.

While many countries have issued indictments related to cyber espionage activity, the most serious cases usually involve foreign actors in countries that are not subject to extradition. As such, law enforcement agencies often are powerless to pursue cybercriminals, particularly those operating abroad.

The 2016 presidential election in the United States made global audiences aware of the danger that can be done by on-line actors. The combined effects on the election will never be known, but their efforts are well understood. Government intelligence agencies worked to undermine the Democratic Party and Democratic candidates led by presidential nominee Hillary Clinton, while activists related to governments and independent merchants selling fake or exaggerated news for click-rates worked to support the resolve of Republican supporters. The idea that foreigners should not intervene in democratic politics of their countries suddenly seemed quant.

Current Dangers

Cyber-attacks have been attributed to governments, criminal entrepreneurs, rebels and even terrorist organizations.[2] Below are some prominent examples of attacks designed to disrupt information networks, access critical materials, destroy data, or mislead the public of various states that have happened in the past year.

Blog: www.pentestpartners.com
LIVE HACK
LIVE HACK
SIXTH ANNUAL CYBERSECURITY SUMMIT
SIXTH ANNUAL CYBERSECURITY SUMMIT
TREND MICRO

States, businesses and individuals are losing huge sums of money to cybercrime. Rebel movements, war lords and terrorists are using the internet to propagandize, intimidate and organize, And democracies are seeing their political systems undermined by rival states and even by individual entrepreneurs in search of clicks from vulnerable voters. Examples of recent attacks include:

- Exchange hack from early 2021 and the compromise of more than 100,000 servers worldwide.
- January 2021. Hackers linked to Hezbollah breached telecom companies, internet service providers, and hosting providers in Egypt, Israel, Lebanon, Jordan, Saudi Arabia, the UAE, Uk, US and the Palestinian Authority for intelligence gathering and data theft.
- February 2021. Suspected Indian hackers targeted over 150 individuals in Pakistan, Kazakhstan, and India using mobile malware, including those with links to the Pakistan Atomic Energy Commission, the Pakistan Air Force, and election officials in Kashmir.
- March 2021. Russian and Chinese intelligence services are suspected of targeting the European Medicines Agency in 2020 in unrelated campaigns, stealing documents relating to COVID-19 vaccines and medicines.
- March 2021. Hackers believed to be related to Chinese government targeted Microsoft software to steal data from over 30,000 organizations around the world, including government agencies, legislative bodies, law firms, defense contractors, infectious disease researchers, and policy think tanks.
- April 2021. New York City's Metropolitan Transportation Authority

[2] Worrall, Willia. 2020. 'Largest breaches and hacks of 2020, the year of the digital pandemic', *Hacked*, 16 December 2021, https://hacked.com/largest-breaches-and-hacks-of-2020-the-year-of-the-digital-pandemic/

(MTA) was hacked by Chinese-backed actors. They were unable to gain access to user data or information systems.

- May 2021. The US FBI and the Australian Cyber Security Centre warned of the Avaddon ransomware campaign targeting multiple sectors in various countries. The reported targeted countries are Australia, Belgium, Brazil, Canada, China, Costa Rica, Czech Republic, France, Germany, India, Indonesia, Italy, Jordan, Peru, Poland, Portugal, Spain, UAE, UK, and the US. The targeted industries include: academia, airlines, construction, energy, equipment, financial, freight, government, health, IT, law enforcement, manufacturing, marketing, retail, pharmaceutical.

- May 2021. The Colonial Pipeline, the largest fuel pipeline in the United States, was the target of a ransomware attack. The energy company shut down the pipeline and later paid a USD 5 million ransom. The attack is attributed to DarkSide, a Russian speaking hacking group.

- July 2021. The United States, the European Union, NATO and other world powers released joint statements condemning the Chinese government for a series of malicious cyber activities. They attributed responsibility to China for the Microsoft

The role of the UN

Internet security has been a major international issue since the internet went public in 1992. It became a major topic for the UN in 1998, when the General Assembly passed its first resolution asking for universal Internet access.[3] That resolution first saw the need to balance the opportunities of the internet with managing the dangers. Back then, the major worry was outsiders attack member States, ‘to prevent the misuse or exploitation of information resources or technologies for criminal or terrorist purposes…’ Back in that innocent time, that first resolution did not consider the possibility that Member States might use the internet to attack the security of other states.

In 2018, the General Assembly’s First Committee requested the Secretary General support a Group of Governmental Experts (GGE), to be established in 2019, pursuant to operative paragraph 3 of General Assembly resolution 73/266:

> to study how to promote common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence -building measures and capacity-building, as well as how

[3] UN. ‘Developments in the field of information and telecommunications in the context of international security, General Assembly resolution 53/70’, United Nations General Assembly, 4 December 1998, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf

> international law applies to the use of information and communications technologies by States, and to submit a report on the results of the study, including an annex containing national contributions of participating governmental experts on the subject of how international law applies to the use of information and communications technologies by States, to the General Assembly at its seventy-sixth session.

Alongside the GGE, the General Assembly also established an Open-Ended Working Group (OEWG). This was open participation from all UN Members States to address the same issues (General Assembly resolution 73/27 of 2018). Russia led the initiative to create the OEWG, which produced its report in March, together with a compendium of statements by States explaining their position on the final report and a Chair's Summary. However, the OEWG failed to address the applicability of international law in cyberspace. As a result, all eyes were then focused on the more ambitious GGE Report.

The GGE Report was completed and published on 10 March 2021. The body overcame the opposition in previous GGEs, and at a time when tensions were high due to the frequency and severity of hostile cyber operations targeting fellow GGE members. Attacks were ranging from persistent election interference to espionage of unprecedented scale like the SolarWinds incident. The 2019-2021 GGE managed to resurrect the most inclusive process by which states consider how international law applies in cyberspace. It does not make specific recommendations for action, but shows the kind of agreement that might be possible.[4]

The GGE recognized the significant of international law in cyberspace, as well as non-binding norms. It began the process of establishing a framework for responsible behavior in cyberspace. Over time, some of the norms are likely to be recognized as the binding law that many States consider them. Those that are not already binding law may eventually crystallize into customary international law or authoritative interpretations of existing rules. States reached the following conclusions and recommendations, which include concrete actions and cooperative measures to address ICT threats and to promote an open, secure, stable, accessible and peaceful ICT environment.

The GGEs Report focus on recommendation for further progress on:

- Identifying and agreeing on existing and potential threats,
- Creation of international rules, norms and principles for responsible state behavior
- Establishing the role in cyberspace of international law,
- Confidence Building Measures (CBMs) to reduce tensions between states,
- Capacity Building for internet security *within* states

Along with these goals, the GGE process made major steps to promoting dialogue between governments, helping them appreciate what is possible and what can be done in the short term to reduce cyber security problems. The conclusions of the GGE report are not binding on the Member States. A major role of these committees is allowing state officials to speak and listen to diverse perspectives, to appreciate each other's perspectives, to hear new ideas and proposals were put forward even when they were not agreed by all States.

[4] Ellen Nakashima and Joseph Marks, 'Russia, U.S. and other countries reach new agreement against cyber hacking, even as attacks continue', *Washington Post*, 12 June 2021, https://www.washingtonpost.com/national-security/russia-us-un-cyber-norms/2021/06/12/9b608cd4-866b-11eb-bfdf-4d36dab83a6d_story.html

The most recent General Assembly resolution on the topic, resolution 75/31, is vague, showing the limits of what can be achieved among suspicions and disagreeing states. It encourages support for the GGE process, but reserving specific recommendations for action. Resolution 75/31 passed by a vote of

- 163 in favor,
- 10 against: Burundi, China, Cuba, Democratic People's Republic of Korea, Iran (Islamic Republic of), Nicaragua, Russian Federation, Syrian Arab Republic, Venezuela (Bolivarian Republic of), Zimbabwe, and
- 7 abstentions: Belarus, Cambodia, Egypt, Lao People's Democratic Republic, Lebanon, Myanmar, Palau.[5]

A meeting of the Group of Government Experts (GGE) on cyber security at the UN in Geneva. Photo: United Nations.

Country and Bloc positions

Positions in the UN on internet and cyber security issues are difficult to understand at face-value. There is a problem of what countries do visibly and what they conceal. Many major actors have—in effect—two internet security polices: a *declaratory* or *formal policy* which they stress in UN diplomacy, and a *covert action policy* that guides their own intelligence agencies and contractors.

All Member States want access internet for official, commercial and personal activity. And they want that made safer. But many also want to preserve intelligence access and freedom to intervene—often covertly—in the networks of other countries. Member States often also want to preserve or enhance their ability to monitor activity in their own countries, ostensibly to track what opposition leaders, rebels and terrorists are using the internet.

This dualism makes it hard for them to seek clearly or act readily. Policies may be worded vaguely or loosely, allowing the wiggle room states need to protect both sides of their activity.

UN negotiators will find that agreement is easy when it is vague, focusing on general principles that everyone supports. But matters become contentious as specific issues of national control and ways of using the internet gain emphasis.

Non-Aligned Movement (NAM): The 120 Member States of the UN's largest voting bloc tend to be internet consumers, relying on internet access provided by companies and servers located elsewhere. This makes them dependent and vulnerable malicious activity. They worry about hacking, ransomware, or other attacks, but even more about basic issues of access and dependence.

Above all, many NAM Member States want assurances than any reforms or national initiatives elsewhere will not limit their freedom

[5] United Nations. 2020. *Advancing responsible State behaviour in cyberspace in the context of international security, A/RES/75/31*, New York: General Assembly, 2020, https://undocs.org/en/A/RES/75/31 Also see the semi-official summary of the General Assembly's deliberations, 'General Assembly, adopting 66 First Committee texts, calls on states to revitalize stalled disarmament machinery, tackle chronic, emerging security threats', *UN General Assembly*, 7 December 2020, https://www.un.org/press/en/2020/ga12296.doc.htm

to use the internet. They generally agree to security-minded reforms, but are likely to demand development aid or relocation of serve farms to their territory in exchange. NAM Member States also want to ensure that their governments can use the internet to enhance national domestic security. They may demand guarantees that their security agencies and domestic contractors can monitor the activity of their own people. Many—but not all—NAM states also are willing to extend international law to include cyber security, giving them something in common with China and most Western countries.[6]

Many Latin American and some African countries are especially likely to cooperate with Western Member States (Australia, Europe, Japan, New Zealand and North America) to develop universal normative principles to guide international agreement on what is allowed and not allowed, on priorities for action.

China: Cyber security may be the issue that divides China most from Russia. On most issues in the UN, the two cooperate, but not cyber security.[7] For China, cyber security means balancing national sovereignty—the right to do as it pleases—with the importance of universal international law. China strongly supports efforts to extend bring international law, including humanitarian law, to cyber activity.

Chinese officials stress that 'The international community should abide by the purposes and principles of the UN Charter, in particular 'the principles of sovereign equality, prohibition of the use of force, non-interference in internal affairs, and peaceful settlement of disputes.' While China seeks to ensure sovereign national control of the internet within their territory, free from interference from foreign countries or firms, it hopes the UN can establish standards that all member States can abide.[8]

The European Union (EU) is especially concerns with free and universal access to the internet, and preservation of individual rights to access and personal privacy. Above all, the EU seeks to ensure that the internet cannot be used for malicious or criminal purposes. Insulation from attacks, protection of user privacy and security are essential.

European countries are willing to accept reduced service standards—including slower service and longer waiting—if it enhances the security and privacy of the system. For Europe, progress must come through international law. In recent years, the demand allowed Europe to develop a loose alliance—on this issue only—with China, which also favors progress through international law.[9]

Russia: Unlike China and much of the NAM, on cyber security issues Russia is widely seen as a spoiler, happy to go it alone in the UN. Russia prefers to slow or stop international action rather than permit the establishment of new international rules that might weaken its freedom of action.

[6] Schmitt, Michael. 2021. 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security*, 10 June 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

[7] Schmitt, Michael. 2021. 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security*, 10 June 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

[8] Liu Yinmeng and Minlu Zhang. 2021. 'China's UN envoy calls for 'equal footing' in cyberspace, *China Daily Global*, 30 June 2021, https://global.chinadaily.com.cn/a/202106/30/WS60dbba2aa310efa1bd65ec48.html

[9] Schmitt, Michael. 2021. 'The Sixth United Nations GGE and International Law in Cyberspace', *Just Security*, 10 June 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

Russia supports its own draft resolutions that stress its national sovereignty, its freedom of action in the cyber domain, and leaves no room for international action or global principles. Critics say Russia will do anything—like extending debate indefinitely or finding trivial reasons to halt action—if it serves its purposes.[10]

United States: American policy in the UN waivers, depending on domestic politics. Under President Trump, the United States made demand for other countries to crack down on cyber-criminal and terrorists within their borders. But the United States refused to permit specific criticism of any particular states harboring attackers, trying to avoid criticism of Russia above all.

That has changed under President Biden. Now the United States strongly supports progress toward global standards of action through global international law. On cyber issues, in the UN it usually cooperates with withs allies in Europe and Asia, and with many Latin American states as well. In the past—during the Trump years—the United States stressed its unilateral advances and freedom of action, but now it seems more willing to accept limits on sovereignty to achieve its goals cooperatively, and more willing to lead.[11]

Some Proposals for Action

Cyber security is vast field. The member States of the UN might choose to focus on a small part of it, or everything. It is up to them. When differences are especially hard to overcome, the General Assembly actually has gone so far as to pass two rival resolutions, based on competing principles. This approach allows all sides to emerge with a modest victory, although it obviously undermines global unity and norm building.[12]

The General Assembly cannot make international law by itself. But it can establish principles and norms to guide the behavior of states. Similarly, the General Assembly cannot force sovereign Member States to do anything. But it can create processes where Member States begin to alter their attitudes and actions. The Member States of the UN are sovereign, free to agree on their own response, including no response at all.

[10] Gold, Josh, 2020. 'Competing U.S.-Russia cybersecurity resolutions risk slowing UN progress further', *Council on Foreign Relations*, 29 October 2020, https://www.cfr.org/blog/competing-us-russia-cybersecurity-resolutions-risk-slowing-un-progress-further ; Sherman, Justin, and Mark Raymond. 2019. 'The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom', *Washington Post*, 4 December 2019, https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/ ; and Vavra, Shannon. 2019. 'The U.N. passed a resolution that gives Russia greater influence over internet norms', *Cyberscoop*, 18 November 2019, https://www.cyberscoop.com/un-resolution-internet-cybercrime-global-norms/

[11] Prince, Todd. 2019. 'U.S. Concerned Russia-Backed UN Resolution Will Hurt Online Freedom', *Radio Free Europe*, 20 December 2019, https://www.rferl.org/a/us-russia-internet-un/30335318.html ; and Nakashima, Ellen, and Joseph Marks. 2021. 'Russia, U.S. and other countries reach new agreement against cyber hacking, even as attacks continue', *Washington Post*, 12 June 2021, https://www.washingtonpost.com/national-security/russia-us-un-cyber-norms/2021/06/12/9b608cd4-866b-11eb-bfdf-4d36dab83a6d_story.html

[12] Gold, Josh, 2020. 'Competing U.S.-Russia cybersecurity resolutions risk slowing UN progress further', *Council on Foreign Relations*, 29 October 2020, https://www.cfr.org/blog/competing-us-russia-cybersecurity-resolutions-risk-slowing-un-progress-further

Some possible paths for UN action include:

Create a new Group of Government Experts (GGE): When the UN is uncertain or cannot agree, creating a committee to further study the issue is an easy alternative. It ensures there will be no need to make decisions for a year or two, while waiting for the committee to report. The key is the mandate for the committee, what the authorizing resolution requires. Who are the committee panelists? They can be independent experts appointed by the UN Secretary-General, but that means member States lose control. Or they can be government - appointed experts who represent selected Member States. The latter is a way to be sure the report will cause no embarrassment.

Prohibit specific uses of the Internet: The General Assembly cannot tell states what to do, but it can agree on standards that all countries are expected to accept. The principles could stress actions that are prohibited, such as hacking foreign networks, denial of service attacks, or destructive uses of networks. For Member States, such steps would mean giving up rights they currently have under international law, which barely covers this domain. But there might be agreement that everyone benefits when such rights are sacrificed. The difficulty is such steps could be viewed by some UN Member States—maybe China, certainly Russia—as thinly veiled attacks on them.[13]

Limit internet control to sovereign domains: A resolution could permit states to give up international rights to use the internet against other states, while preserving their right to regulate it domestically as they please.

End the distinction between domestic and international behavior in the cyber domain. Rather than having two sets of rules for every country—one domestic rule and another for international behavior—the UN could agree the differences should be eliminated. Domestic rules would be extended to apply to the international conduct. What is prohibited at home—such as hacking, espionage, denial of service attacks or ransomware attacks—would also be banned internationally.

Focus on the action of specific countries or groups. The General Assembly might stress not overall cyber security policy, but isolating for criticism and penalty the actions of specific states. Most likely this would be directing global attention—maybe sanctions—against specific offenders.

Bibliography

Collier, Kevin, 2019. ‘27 countries sign cybersecurity pledge with digs at China and Russia’, CNN< 23 September 2019, https://www.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html

[13] Kevin Collier, ‘27 countries sign cybersecurity pledge with digs at China and Russia’, CNN< 23 September 2019, https://www.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html

Gold, Josh, 2020. ‘Competing U.S.-Russia cybersecurity resolutions risk slowing UN progress further’, *Council on Foreign Relations*, 29 October 2020, https://www.cfr.org/blog/competing-us-russia-cybersecurity-resolutions-risk-slowing-un-progress-further

Liu Yinmeng and Minlu Zhang. 2021. ‘China's UN envoy calls for 'equal footing' in cyberspace, *China Daily Global*, 30 June 2021, https://global.chinadaily.com.cn/a/202106/30/WS60dbba2aa310efa1bd65ec48.html

Nakashima, Ellen, and Joseph Marks. 2021. ‘Russia, U.S. and other countries reach new agreement against cyber hacking, even as attacks continue’, *Washington Post*, 12 June 2021, https://www.washingtonpost.com/national-security/russia-us-un-cyber-norms/2021/06/12/9b608cd4-866b-11eb-bfdf-4d36dab83a6d_story.html

O'Sullivan, Kate. 2021. ‘UN makes critical progress on cybersecurity’, *Microsoft*, 29 March 2021, https://blogs.microsoft.com/on-the-issues/2021/03/29/un-working-group-cybersecurity-report/

Prince, Todd. 2019. ‘U.S. Concerned Russia-Backed UN Resolution Will Hurt Online Freedom’, *Radio Free Europe*, 20 December 2019, https://www.rferl.org/a/us-russia-internet-un/30335318.html

Schmitt, Michael. 2021. ‘The Sixth United Nations GGE and International Law in Cyberspace’, *Just Security*, 10 June 2021, https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/

Sherman, Justin, and Mark Raymond. 2019. ‘The U.N. passed a Russia-backed cybercrime resolution. That’s not good news for Internet freedom’, *Washington Post*, 4 December 2019, https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/

UN, 1998. ‘Developments in the field of information and telecommunications in the context of international security, General Assembly resolution 53/70’, United Nations General Assembly, 4 December 1998, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf

UN, 2020. *Advancing responsible State behaviour in cyberspace in the context of international security, A/RES/75/31*, New York: General Assembly, 2020, https://undocs.org/en/A/RES/75/31

UN, 2020. General Assembly, adopting 66 First Committee texts, calls on states to revitalize stalled disarmament machinery, tackle chronic, emerging security threats’, *UN General Assembly*, 7 December 2020, https://www.un.org/press/en/2020/ga12296.doc.htm

Vavra, Shannon. 2019. ‘The U.N. passed a resolution that gives Russia greater influence over internet norms’, *Cyberscoop*, 18 November 2019, https://www.cyberscoop.com/un-resolution-internet-cybercrime-global-norms/

Worrall, Willia. 2020. ‘Largest breaches and hacks of 2020, the year of the digital pandemic’, *Hacked*, 16 December 2021, https://hacked.com/largest-breaches-and-hacks-of-2020-the-year-of-the-digital-pandemic/