ODUMUNC 2023 Issue Brief
UN Security Council

Cybersecurity and Its Potential Threats

by Mario A Pico
Old Dominion University

Introduction

What should be role of the United Nations governing use of the internet.? Does it set *standards for freedom* of speech and access? Or does it protect the interests of its 193 Member States? Does it protect the internet and individual users, or does it *serve state interests* to use the internet as governments wish? These are questions for the United Nations to decide.

The internet and technologies that connect people to one another have spurred transformative growth for nations all over the world. Social media technologies not only allow us to speak to friends and family but they morphed into tools that improve efficiency and productivity in the workplace, allowing people the world over to enjoy a more harmonious work/life balance. They allowed for the digitization of important documents such as medical records, financial statements, state legislations along the ability to securely store and transfer those digital documents. Simply put, Information Communication Technologies (ICTs) have vastly improved opportunities for human progress and global cooperation between private and public entities alike.

Unfortunately, these technologies are only one side of a very large coin—where one side promotes positive development and progress (economic, societal), the other harbors the ability to use the same technologies against us. The misuse of these technologies affects the regular citizen, private corporations, and states alike. Reactions by states to counter this misuse has wide ranging responses—from doing little to nothing at all, to creating heavy handed legislation that violates human rights. But simply because some states do little to nothing does not mean they do not care about cybersecurity, but that they do not have the means or resources to effectively counter the problem. It is in the international community's best interest to narrow the digital divide and bridge the gap with the assistance from nations with capacity to handle these threats to those who lack that ability.

Background

Cybersecurity encompasses more than just installing your preferred anti-virus software. It requires training and understanding of the methods that are used to attack organizations or individuals. This includes hiring professionals to install, manage, and monitor the infrastructure and tools used to defend their respective networks. Networks are as strong as their weakest link, and if users do not have basic fundamental awareness of cybersecurity, it leaves those networks vulnerable to compromise.

Cybercriminals use ICTs to deliver spam to individuals personal e-mail inboxes in the hopes an unsuspecting victim would click on a link that could download malware or send them to a site pretending to be legitimate with the intent for the victim to enter their credentials and other information. The same risks apply to corporations and governments. Any unsuspecting individual can fall victim to these sorts of phishing attacks, where the results could lead to catastrophic consequences. Misuse of ICTs does not stop there.

Malware has been developed so it that can wipeout entire digital data repositories[1], spy on and track its victims[2], hold entire institutions at ransom[3], and effectively destroy physical infrastructure. These are some of the most notable examples of cyberattacks allegedly perpetrated by state-actors and criminal groups. It is important to differentiate between cybercrime and cyberwarfare and their potential motives, but to also note that criminal groups and state-actors' interests may align. In many cases, governments would seek to avoid direct involvement, and would sponsor groups to do its bidding.

In 2007, Estonia became the first country to fall victim to a highly publicized massive cyberattack that targeted multiple institutions throughout its society. All of its government websites, infrastructure, political party websites and some banking websites were defaced and inaccessible through what is known as Distributed Denial of Service (DDoS) attacks. DDoS is defined as distributed, meaning it requires the usage of multiple systems (that are distributed) to overwhelm targeted networks/servers with the goal of crippling them. The Estonian government laid blame on the Russian Federation (RF), but no credible evidence was discovered to apply attribution to Russia.[4]

In the years 2009-2010, the Iranian Nuclear Fuel Enrichment Plant at Natanz was a target of a sophisticated computer worm, Stuxnet, which was specifically developed to find and destroy particular equipment within the facility. A malicious computer worm requires little to zero human interaction for it execute and replicate itself, perhaps other than the effort required to deliver the malware to the desired target. It is understood that Stuxnet was delivered into the facility via USB drive, where an insider, or unsuspecting engineer plugged the drive into a computer on the internal network. The worm replicated and hid itself within the network, searching for the target hardware and software. Once it infected the appropriate systems, it waited for certain criteria to be met before executing its payload. While Stuxnet was effectively destroying centrifuges in the Natanz facility, any engineer monitoring that equipment did not know it due to the malware sending data to make the centrifuges appear is if they were operating normally. [5]

The attribution of this attack is believed to be that of intelligence agencies from the United States (US) and Israel, although neither has ever claimed responsibility for the attack.

In 2021, there was series of cyberattacks against critical oil infrastructure and a food processor. Colonial Pipeline, an American oil pipeline, and JBS S.A., a Brazilian based meat processing company, both suffered ransomware attacks in the same month. Ransomware is a type of malicious malware that once it infects a host or network, it locks out users and prompts them to pay the attacker a ransom, usually in cryptocurrency. Colonial Pipeline's billing system was compromised, and that lead to the decision to shut down the pipeline over concerns that the processor would not be able to bill

[1] Christopher Bing et al., "Ukraine Computers Hit by Data-Wiping Software as Russia Launched Invasion," Reuters (Thomson Reuters, February 24, 2022), https://www.reuters.com/world/europe/ukrainian-government-foreign-ministry-parliament-websites-down-2022-02-23/

[2] Ronen Bergman and Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon," The New York Times (The New York Times, January 28, 2022), https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

[3] "Cyber Attack 'Most Significant on Irish State'," BBC News (BBC, May 14, 2021), https://www.bbc.com/news/world-europe-57111615

[4] Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," Digital Commons @ University of South Florida (Journal of Strategic Security, June 9, 2011), https://digitalcommons.usf.edu/jss/vol4/iss2/4/

[5] David Kushner, "The Real Story of Stuxnet," IEEE Xplore (IEEE, March 7, 2013), https://ieeexplore.ieee.org/document/6471059

customers appropriately for the oil they would receive.[6] The perpetrators of this attack were a criminal group called DarkSide, who self-proclaim to be apolitical and not seeking to shape geopolitics.[7]

In the JBS S.A. cyberattack, the companies' American subsidiary, JBS USA and all of its North American facilities were temporarily taken offline by ransomware. The attack also affected facilities in Australia. This incident highlighted the vulnerabilities in the food processing industry that simply go beyond being unprepared for cyberattacks.[8] The group reportedly responsible for the attack was called REvil, but they never claimed themselves responsible. Although not having any formal affiliation with the Russian Federation, US President Joe Biden informed Russian President Vladimir Putin that the organization responsible was Russian in origin and he expected the Russian government to take action against them.[9]

The issues that arise due to cyberattacks, is that eventually, if not immediately, regular citizens will fall victim to the downstream effects. In the case of JBS USA, service was restored within 72 hours. With the size of JBSs operation, any longer could mean that meat products would not get to supermarkets or grocers. JBS capitulated and paid the ransom to unlock its system, but this does not necessarily bode a good outcome. The issue with this action is that victims never know if they will actually get back full control of their system. Good practice would be to have backups ready to restore your data, or even better, secondary sites that can go online in the event of disaster.

These consequences can be worse for more upstream infrastructure, like energy. If a major energy provider were to fall victim to a cyberattack that reduced or completely shut off service to a region, country, or countries, hundreds of thousands to millions of people would be affected. With no electricity to power life-sustaining medical devices, chill their food, or control the climate of their homes especially during summer and winter months, people could suffer adversely or even perish.

Issues

Fundamental disagreements between major powers still hinder progress in the advancement of peace and security in cyberspace. Although broad consensus was reached in the UN's Cybersecurity Open Ended Working Group (OEWG) on its language and recommendations, it fell short of addressing root causes of global cyber instability.[10] These current issues are comprised of known problems like inadequate protections for civil society in cyberspace and the infrastructure they rely on for their daily lives. Social media is also a vector for cyberattacks. With an estimated 4.59 billion people using some form of social media in 2022,

[6] Natasha Bertrand et al., "Colonial Pipeline Did Pay Ransom to Hackers, Sources Now Say | CNN Politics," CNN (Cable News Network, May 13, 2021), https://edition.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html

[7] David E. Sanger and Nicole Perlroth, "F.B.I. Identifies Group behind Pipeline Hack," The New York Times (The New York Times, May 10, 2021), https://www.nytimes.com/2021/05/10/us/politics/pipeline-hack-darkside.html

[8] Jacob Bunge, "Lawmakers Scrutinize Meatpacking as JBS Rebounds from Cyberattack," The Wall Street Journal (Dow Jones & Company, June 4, 2021), https://www.wsj.com/articles/concerns-over-meat-supply-ebb-as-jbs-plants-reopen-after-cyberattack-11622718004?mod=searchresults_pos4&page=1

[9] Zeke Miller, "Biden Tells Putin Russia Must Crack down on Cybercriminals," AP NEWS (Associated Press, July 9, 2021), https://apnews.com/article/joe-biden-europe-technology-government-and-politics-russia-df7ef73f02bcba61ad6e628aa95a9f84

[10] Arindrajit Basu, Irene Poetranto, and Justin Lau, "The UN Struggles to Make Progress on Securing Cyberspace," Carnegie Endowment for International Peace, May 19, 2021, https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491

and that number expected to grow close to 6 billion in 2027, it would be the fastest growing and possibly largest attack surface.[11]

Through the use of social engineering over social media, threat actors can fool users into giving up account names and passwords or other Personal Identifiable Information (PII). These attacks do not only leave society at risk from cybercriminals who wish to gain financially or for simple thrill-seeking, but from state and state sponsored threat actors. Social media can also be used to spread misinformation and sow discontent. Western liberal democracies in Europe and the United States tend to favor a more open and permissive internet, which leaves their societies susceptible to misinformation. Throughout the COVID-19 Pandemic, medical misinformation ran rampant over social media, and companies struggled to keep up with and police the proliferation of this phenomena.

The usage of social media to spread discontent and misinformation is no new phenomena. Facebook was used as a vector to spread hate speech which led to ethnic violence against the Rohingya Muslim minority in Burma (Myanmar) by the Burmese military from 2016 to 2017. The United Nations has accused the Burmese military of committing genocide against the minority population, where hundreds of thousands were displaced, and tens of thousands were beaten, raped, and killed.[12][13] For its part in the matter, Facebook admitted it played a role in inciting the violence against the Rohingya, given the violent rhetoric was prolifically spread through advertisements on its platform. There still remains total lack of accountability for these atrocities, with total disregard to human rights and International Humanitarian law.

The lack accountability of states and the trend to deemphasize human rights with regards to the internet remain priority issues that should be solved. Additionally, emerging disruptive technologies like artificial intelligence (AI) and quantum computing pose both to be a challenging threat and tools for progress. The misuse of ICTs leads to mistrust between states which further erodes cooperation and increases tension and risk of conflict, placing societies at risk.

Leading Countries and Positions

The People's Republic of China (PRC) and the United States largely view the internet and the information domain as imperative to their national and economic security, while viewing one another as their primary competitor if not an adversary. The Russian Federation seeks to remain relevant on the world stage and will use "Active Measures" to tip the scales in other countries internal affairs by influencing electoral outcomes and manufacturing outrage into their discourse. The European Union's (EU) aim is to be a leader in cyberspace while promoting resilience to safeguard data and communications while keeping a free and open internet.

The People's Republic of China. China maintains a position domestically to what is referred as "internet sovereignty", meaning that it maintains the right to regulate ICTs and associative activities within its territory, and extends that belief to other states as well.

[11] S. Dixon, "Number of Worldwide Social Network Users 2027," Statista, September 16, 2022, https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

[12] Associated Press, "U.N. Genocide Advisor: Myanmar Waged 'Scorched-Earth Campaign' against the Rohingya," Los Angeles Times (Los Angeles Times, March 14, 2018), https://www.latimes.com/world/la-fg-myanmar-rohingyas-20180313-story.html

[13] Moshin Habib et al., "Forced Migration of Rohingya: The Untold Experience," ResearchGate (Ontario International Development Agency, August 2018), https://www.researchgate.net/figure/Forced-Migration-of-Rohingya-The-Untold-Experience_fig1_326912213

Internationally it pushes for capacity building, reporting of vulnerabilities by states and secure ICT supply chains. Internationally, it is less well-known for offensive attacks than Russia, but uses cyber-attacks largely for espionage on its own people abroad, on foreign companies, groups and governments.

China believes that following norms, rules and principles should be observed and states should prioritize peace, security, openness, cooperation and order in cyberspace. Furthermore, it believes states should not use ICTs in ways that are inconsistent with maintaining international peace and security.[14] The PRC also established the sweeping National Intelligence Law of 2017, and within its language mandates that domestic manufacturers of ICTs submit data to the government for investigative purposes in the interest of national security.[15]

The European Union. The 27 Member States of the EU take a significantly comprehensive view towards cybersecurity. It fundamentally understands the risks posed by ICTs and realizes that cybersecurity is now a societal need. It has established governing agencies like the European Union Agency for Cybersecurity (ENISA) and established policies like the NIS Directive that set strict reporting standards for digital service providers and operators of essential services. Major legislation includes the EU Cybersecurity Act which establishes a certification framework for ICTs within the EU, and a robust data privacy law, the General Data Protection Regulation (GDPR). Internationally, the EU aims to cooperate and build capacity with third countries to help them defend against threats posed to cybersecurity.[16][17][18]

The Non-Aligned Movement (NAM). The 120 Member States of the UN's largest voting bloc, generally known as the NAM, historically sought to remain neutral in the geopolitical competition between the major powers like the PRC and the US. Although some members have preferred partners with regards to economic and defense strategies, the movement still seeks to prioritize peace and stability. Speaking for the NAM, Indonesian's representative stated that cyberspace should never become a theatre of military operations, and all efforts should be made to avoid it becoming a conflict area. Other members of the movement, specifically from the Caribbean Community stressed that given their economic situations, challenges with violent crime, and vulnerability to natural disasters makes it less likely for them to shift resources to other emerging threats and issues like cybersecurity. States in the NAM would seek partnership and cooperation with other states and NGOs to develop capacity.[19]

The Russian Federation (RF). The RF has long been one of the leading advocates for establishing norms with regards to the use of ICTs. Russia is well known to use the internet for cyber-attacks, including malware and denial

[14] FMPRC, "China's Positions on International Rules-Making in Cyberspace," Ministry of Foreign Affairs of the People's Republic of China, October 20, 2021, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html

[15] Arjun Kharpal, "Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have a Choice," CNBC (CNBC, March 5, 2019), https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html

[16] "Cybersecurity - Our Digital Anchor - A European Perspective," EU Science Hub, n.d., https://joint-research-centre.ec.europa.eu/crosscutting-activities/facts4eufuture-series-reports-future-europe/cybersecurity-our-digital-anchor-european-perspective_en

[17] "The EU Cybersecurity Act," Shaping Europe's digital future, n.d., https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[18] "Cybersecurity Policies," Shaping Europe's digital future, n.d., https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

[19] "Delegates Propose New Programme of Action for Struggle against Threats to Cybersecurity, in First Committee Thematic Debate | UN Press," United Nations (United Nations, October 18, 2021), https://press.un.org/en/2021/gadis3673.doc.htm

of service attacks. Russia initiated the debate on cybersecurity in the UN in the late 1990s, and even proposed the Group of Governmental Experts (GGE) format. The GGE is a small group of national experts that can be convened at the request of the UN General Assembly what will study specific issues in an attempt to find consensus.[20] It has sought to establish norms committed to the Charter of the UN, but maintained emphasis on state sovereignty, state control and non-interference in the information space as imperative behavior between states.[21] The RF has been one of the most active participants in cyberspace, and has been accused of conducting, sponsoring or being the origination point for many of the highest profile cyberattacks in recent memory. The RF is willing to conduct overt attacks to signal to other nations its abilities in cyberspace and the information domain. This strategy is likely due to the aggressive nature of its domestic security and military intelligence agencies. The RF have also shown the capability to conduct covert and long term cyber operations, such as the SolarWinds compromise.[22]

The United States of America (US). The US promotes internet freedom and support for an open, interoperable, secure, and reliable cyberspace. It works to oppose efforts to restrict internet freedoms, or efforts to eliminate the multi-stake holder approach to internet governance.[23] But the US also engages in offensive cyber-attacks, most famously the 2009 *Olympic Games* attack against Iran.

The US believes that an open, secure and stable cyberspace is critical for the success of the global economy. It partners with the private sector to improve the security of ICT supply chains, and harden critical infrastructure. It also seeks to work with international partners to build capacity, develop and establish international norms of behavior in cyberspace, and collaborate in cybercrime investigations. But despite these policies, the internet is becoming more fragmented and less free.[24] The US has yet to sign any formal legislation surrounding cybersecurity or data privacy, and relies largely on Executive Orders and initiative announcements of collaboration with the private sector.

The Role of the United Nations

The United Nations has recently adopted two resolutions with regards the security of ICTs, A/RES/73/27[25] and the advancement of responsible state behavior in cyberspace, A/RES/73/266[26]. Resolution 73/27, sponsored

[20] "Group of Governmental Experts – UNODA," United Nations (United Nations, n.d.), https://www.un.org/disarmament/group-of-governmental-experts/

[21] Elaine Korzak, "Russia's Cyber Policy Efforts in the United Nations - CCDCOE," CCDCOE (CCDCOE, 2021), https://ccdcoe.org/uploads/2021/06/Elaine_Korzak_Russia_UN.docx.pdf

[22] David E. Sanger, Nicole Perlroth, and Julian E. Barnes, "As Understanding of Russian Hacking Grows, so Does Alarm," The New York Times (The New York Times, January 2, 2021), https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html

[23] The White House, "Foreign Policy Cyber Security," National Archives and Records Administration (National Archives and Records Administration, n.d.), https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity

[24] Adam Segal, "A New U.S. Foreign Policy for Cyberspace," Council on Foreign Relations (Council on Foreign Relations, July 12, 2022), https://www.cfr.org/blog/new-us-foreign-policy-cyberspace

[25] United Nations, "Developments in the Field of Information and Telecommunications in the Context of International Security," General Assembly Resolution A/RES/73/27 (New York: United Nations, December 11, 2018), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement

[26] United Nations, "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security," General Assembly Resolution A/RES/73/266 (New York: United Nations, January 2,

by the Russian Federation, established the OEWG on security of ICTs that comprised the entire UN membership, with the goals of making negotiations more transparent, democratic and inclusive. It sought to further develop rules and norms of responsible behavior of states, how to implement them, and change them if necessary. It also mandates for the body to continue to study potential threats to information security and what cooperative measures can address them, how international law applies to the usage of ICTs by states, and to how to build confidence and capacity building. The voting summary for this resolution was 119 Y, 46 N, 14 abstentions, 14 non-voting.

Resolution 73/266, sponsored by the United States, established another GGE that is comprised of only 25 member states. The group would continue to study possible cooperative measures for addressing new and existing threats to ICTs, the norms, rules and principles of responsible state behavior, confidence-building measures, capacity building, and how international law applies to the state use of ICTs. The voting summary for this resolution was 138 Y, 12 N, 16 abstentions, 27 non-voting.

The United Nations has currently taken a parallel approach to the study of cybersecurity and ICTs with the dual establishment of the OEWG and GGE formats. So far, no decisive resolutions have been made with regards to cybersecurity/ICTs, and how states should use them responsibly. The consensus so far has been that more studying and research should be done to present a more informed solution.

The United Nations should take a more proactive role in moving forward with establishing the rules and norms of responsible state behavior with regards to the use of ICTs. It should prioritize human rights with the integration of International Humanitarian Law into any future resolutions. Integration of International Humanitarian Law is of paramount importance, as it is designed to protect civilians during armed conflict. The UN should seek the disarmament/demilitarization of cyberspace, and strive to establish mechanisms to hold states accountable for actions that harm international peace, security and stability.

2019), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement

Bibliography

Basu, Arindrajit, Irene Poetranto, and Justin Lau. "The UN Struggles to Make Progress on Securing Cyberspace." Carnegie Endowment for International Peace, May 19, 2021. https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491

FMPRC. "China's Positions on International Rules-Making in Cyberspace." Ministry of Foreign Affairs of the People's Republic of China, October 20, 2021. https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/20211020_9594981.html

United Nations. "Advancing Responsible State Behaviour in Cyberspace in the Context of International Security." General Assembly Resolution A/RES/73/266. (New York: United Nations, January 2, 2019). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement\

United Nations. "Developments in the Field of Information and Telecommunications in the Context of International Security." General Assembly Resolution A/RES/73/27. (New York: United Nations, December 11, 2018). https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/418/04/PDF/N1841804.pdf?OpenElement

The White House. "Foreign Policy Cyber Security." National Archives and Records Administration. National Archives and Records Administration, n.d. https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity

"Cybersecurity - Our Digital Anchor - A European Perspective." EU Science Hub, n.d. https://joint-research-centre.ec.europa.eu/crosscutting-activities/facts4eufuture-series-reports-future-europe/cybersecurity-our-digital-anchor-european-perspective_en