Forum: General Assembly (GA)

Question of: Ensuring international peace and security in cyberspace

Student Officer: Layla Jo-Won Cyhn, Deputy Assistant President

Introduction

The publisher database IGI Global defines cyberspace as “the global electronic web of people, ideas, and interactions on the Internet…unencumbered by the borders of the geopolitical world.” The boom of mobile phones, computers, and other devices provides global connectivity, but also facilitates a modern plethora of cyberattacks endangering stability and sustainable development. Furthermore, in recent years, numerous terrorist organizations have turned to the cyber sphere to spread harmful propaganda, collect critical resources, and attack technology-based structures, such as hospitals, water supplies, energy systems, and more.[1] Therefore, as the technology sector continues to expand and develop into human life and activity, finding suitable defenses against online attacks should become a top priority. Cybercrime is a contemporary offense, but one that must be addressed by the international community to prevent a collapse of the digital space that pillars global activity. Delving into this agenda will prompt delegates to consider ways that personal, national, and international security can extend not only to physical, but digital manifestations as well.

The idea of using informational architecture over combat in the real world has been present long before modern electronics were invented. In fact, historians believe that the first record of cybercrime dates all the way back to 1834, when a pair of thieves hacked into the French telegraph system and stole confidential information on the financial market.[2] As technology developed over the years, including products such as Alexander Graham Bell’s telephone and Charles Babbage’s first mechanical computer, more people started to realize they could manipulate these systems to gain entry into confidential places of information. Furthermore, in the early 2000s, social media’s presence began skyrocketing into the global community: criminals could now “work in groups, use well-established tactics, and target everything and anybody with a web presence.”[3]

[1] “Fighting Terror in Cyberspace.” World Scientific. Accessed June 22, 2022. https://www.worldscientific.com/worldscibooks/10.1142/5934.

[2] “Cyber CEO: The History of Cybercrime, from 1834 to Present.” Herjavec Group, September 14, 2021. https://www.herjavecgroup.com/history-of-cybercrime/#:~:text=1834%20%E2%80%94%20French%20Telegraph%20System%20%E2%80%94%20A,conducting%20the%20world's%20first%20cyberattack.

[3] “The History of Cybercrime: A Comprehensive Guide(2021).” Jigsaw Academy, February 13, 2021. https://www.jigsawacademy.com/blogs/cyber-security/history-of-cybercrime/.

Additionally, in the newly modern age, technology has "infiltrated every aspect of our lives…changes how we work, how we learn, and how we shop."[4] In response to this electronic boom, corporations, government organizations, and other groups with confidential information "[recruited] cyber security experts, [upgraded] systems and [innovated] technology…[only to observe] hackers consistently and unsurprisingly stay[ing] one step ahead."[5] Snapchat, Twitter, Facebook, and other social media have continuously experienced breaches in their security by hacks, ransoms, and other cyberattacks, putting their millions of users at risk of identity theft, financial loss, and privacy breaches.[6]

Upon closer analysis, not all hackers have the same motives; some commit cybercrime for financial gain, to spread a message, or even just for fun.[7] But when a nation's security is involved, a common theme emerges: "stealing secrets, gathering cyber intelligence, conducting reconnaissance, or disrupting operations"[8] are just a few of the methods used to undermine a country's stability. These motivations were proven in the 2010 discovery of Stuxnet, a computer worm "specifically written to take over certain programmable industrial control systems and cause the equipment run by those systems to malfunction."[9] The virus, which had reportedly been circulating since early 2009, was originally created to cripple Iran's nuclear factories and actually succeeded in "destroying numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out." Stuxnet's discovery sent the world into a frenzy—the world's very first virus that could destabilize national hardware appeared to have been created by the U.S. National Security Agency, the CIA, and Israeli intelligence.[10] The cybersecurity company Recorded Future's COO, Stu Solomon, commented on the matter: "groups of cybercriminals who aren't sponsored by a government normally will work with the government on various national objectives…to continue their cybercrime." This unusual collaboration stems from many world affairs shifting to digital versions and cyberspace—as the "rise of information warfare" surges, leaders are "investing billions to develop capabilities…and explo[iting] the vulnerabilities of electronic communications networks."[11] But this intense fortification may very well be too little, too late. Brandeis School Professor Anna Scherdina estimates that malicious cyber activity cost the U.S. (alone) between

[4] Published. "The Role of Technology." Knight Foundation, June 10, 2016. https://knightfoundation.org/digitalcitizenship/technology/.

[5] Tripwire Guest AuthorsAug 17, 2016Featured Articles. "The Evolution of Hacking." The State of Security, August 17, 2016. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/

[6] "7 Social Media Sites and Their Data Breaches." humanID, June 21, 2022. https://human-id.org/blog/biggest_social_media_breach_history/.

[7] Watering, J. van de. "The Origin of Cybercrime - Goose VPN." GOOSE VPN service, March 5, 2020. https://goosevpn.com/blog/origin-cybercrime.

[8] "The Final Report on Nobelium's Unprecedented Nation-State Attack." NTSC. Accessed June 23, 2022. https://www.ntsc.org/underwriters/underwriter-blogs/the-final-report-on-nobeliums-unprecidented-nation-state-attack.html.

[9] Encyclopædia Britannica, inc. (n.d.). *Stuxnet*. Encyclopædia Britannica. Retrieved June 24, 2022, from https://www.britannica.com/technology/Stuxnet.

[10] *What is stuxnet?* Trellix. (n.d.). Retrieved June 24, 2022, from https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html.

[11] Stupples, D. (2015, November 27). *The next big war will be digital-and we're not ready for it*. Gizmodo. Retrieved June 24, 2022, from https://gizmodo.com/the-next-big-war-will-be-digital-and-we-re-not-ready-fo-1744865435.

$57 and $109 billion in 2016,[12] and with the rise in technology growing exponentially every year, that figure could very well skyrocket in the decades to come. In fact, according to the company PC World's analysis, the average ransomware demand is $1,077 – "for an individual, that could be the decision between losing all their files, paying the rent, or putting food on the table."[13]

The international community has been grappling with cyber security measures for decades, and the UN General Assembly has created numerous resolutions in response to the growing crisis. In 1999, they tackled the issue of Information and Communications Technology (ICTs) and how its exploitation could destabilize international peace and order—most of their action, however, laid in simplistic "general appreciation of the issues of general security" and "definitions of basic notions related to information security."[14] Nevertheless, in recent years (and as technology's influence in the world more than quadrupled), the UNGA grew to pass a record number of resolutions in regards to "safeguarding privacy in the face of new threats…and protect peaceful assembly and association, both online and offline."[15]

However, two of the committee's member nations in particular continue to draw controversy for their role in historical cyber warfare. The People's Republic of China and the Russian Federation have continuously divided experts as the biggest cyber adversary to the rest of the world. This result originates from years of attacks from both nations, including "Chinese thefts of company secrets that have robbed billions of dollars" and "Kremlin-backed hacks that undermined democratic values and compromised troves of government secrets."[16] With countries fighting to simultaneously become the next world powers in technology and preserve their cybersecurity, the lack of trust among member states has impeded future advancements into the matter at hand. Furthermore, there are no distinct 'cyber-borders' between countries, and existing laws in many countries are often not equipped to handle these threats, something that many criminals take advantage of to conduct crimes that they can get away with online. The complexity of the type, amount, and severity of different cyber crimes can make it difficult for justice systems to process proper sentencing and fight back against the threats. However, as more governments

[12] *How bad are cyberattacks for the economy? This professor helped the White House assess the damage*. How bad are cyberattacks for the economy? This professor helped the White House assess the damage. (n.d.). Retrieved June 24, 2022, from https://www.brandeis.edu/global/news/2020/scherbina-q-a.html.

[13] *How cyber attacks affect individuals and how you can help keep them safe*. ECPI University. (n.d.). Retrieved June 24, 2022, from https://www.ecpi.edu/blog/how-cyber-attacks-affect-individuals-and-how-you-can-help-keep-them-safe.

[14] United Nations. (n.d.). *Developments in the field of information and telecommunications in the context of international security :* United Nations. Retrieved June 24, 2022, from https://digitallibrary.un.org/record/265311?ln=en.

[15] *UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed Outcomes for Human Rights Online*. UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online | Association for Progressive Communications. (n.d.). Retrieved June 24, 2022, from https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed.

[16] Marks, J., & Schaffer, A. (2022, January 20). *Analysis | is Russia or China the biggest cyber threat? experts are split*. The Washington Post. Retrieved June 24, 2022, from https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/.

start to ease into the rapidly expanding digital world, many are calling for an increase in international cooperation to ensure peace online as well as in the physical world[17]

Moving forward, delegates should ask themselves which factors hinder international cooperation and unity in cyberspace, and which procedures may be implemented to foster critical dialogue between nations.

Definition of Key Terms

Cyberspace

The term cyberspace first originated from a 1982 science fiction novel, as a term used to describe "the creation of a computer network in a world filled with artificially intelligent beings"[18]. At the time, this computerized world may have been an exaggeration, but in recent years its image has become increasingly realistic. The Internet has picked up a life of its own; people communicate, shop, trade, and behave in ways that are different online to those of the physical world. The global community invents new "telecommunications networks, computer systems, and embedded processors and controllers in critical industries" every day, to be used in hospitals, schools, urban cities, and more.[19] However, the "marketplace of conflict"[20] that technology can foster has been a point of controversy over the years—the anonymity feature of social media often facilitates online threats, blackmail, and other types of criminal activity from its users.

Cyberattacks

The UN Institute for Disarmament Research (UNIDIR) defines a cyberattack as "the penetration of computers or digital networks" that is "often unauthorized."[21] These threats often manifest in several different predicaments, including but not limited to identity theft, financial security damage, employment or business service complications, and impacting transportation and the power grid, among other effects.[22] However, in an ironic twist, certain companies, organizations, or even entire nations, have purposefully "simulat[ed] large-scale cyber security incidents" in order"to analyze advanced technical cybersecurity

[17] Lovet, G. (2012, September 2). *FIGHTING CYBERCRIME: TECHNICAL, JURIDICAL AND ETHICAL CHALLENGES*. HHS.gov. Retrieved July 19, 2022, from https://web.archive.org/web/20110902091006/http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.

[18] Encyclopædia Britannica, inc. (n.d.). *Cyberspace*. Encyclopædia Britannica. Retrieved June 26, 2022, from https://www.britannica.com/topic/cyberspace.

[19] Editor, C. S. R. C. C. (n.d.). *Cyberspace - glossary*. CSRC. Retrieved June 26, 2022, from https://csrc.nist.gov/glossary/term/cyberspace.

[20] Katsh, M. E. (n.d.). *DISPUTE RESOLUTION IN CYBERSPACE*. Dispute resolution in Cyberspace. Retrieved June 26, 2022, from https://www.umass.edu/legal/articles/uconn.html.

[21] United Nations. (n.d.). *Unidir: The humanitarian impact of cyber attacks against Critical Infrastructure (4 July 2022)*. United Nations. Retrieved June 26, 2022, from https://indico.un.org/event/38035/.

[22] *Cybersecurity*. Cybersecurity | Ready.gov. (n.d.). Retrieved June 26, 2022, from https://www.ready.gov/cybersecurity.

incidents,"[23] proving that in many cases, cyberattacks can even help identify weaknesses in digital fortification. New York Times journalist Charles Henderson commented: "[h]acking is an activity, and what separates any activity from crime is, very often permission"[24]—often, widespread fear of a cyberattack comes from fear that information stolen could be used against the victim in some way. A breach in confidentiality is what endangers lives, rather than a written program or code; and nations have taken to strict jail times, travel bans, and/or the creation of national or multinational task forces to protect themselves against the more malicious of attacks[25].

Cyber Terrorism

The European Union Agency for Law Enforcement Training defines cyber terrorism as "the use of computers and/or related technology with the intention of causing harm or damage," in ways that include "coerc[ing] a civilian" or "influenc[ing] policy of [a] target government."[26] Many people are unaccustomed to threats that take place outside of physical violence, and thereby "unaware of what it means and how dangerous it can be."[27] While bombs, artillery shells, and invasions plaster the news every week, attacks that take place in the cyberspace can be just as dangerous, if not more—proponents of anonymous online communication can make it harder for governments and security forces to locate and eliminate the danger. In all, the Internet can easily foster the "glorification of terrorist acts, incitement to commit acts of terrorism, dissemination of illegal content" facilitati[on of] communication between terrorist actors and the training of potential recruits"[28].

Virtual Private Network (VPN)

Virtual private networks (VPNs) are "services that protect your Internet connection and privacy online" by "creating an encrypted tunnel for your data" and thereby "protecting your online identity."[29] The casual user may use VPN to gain new Netflix titles, or break past their school's WiFi ban on Instagram, but the program has experienced bans in several countries, including China, Russia, Iraq, and Oman. In many cases, according to information technology journalist Timothy Shim, the "legality of VPNs seem directly tied to the type of government in control," in that "governments find it hard to track,

[23] *Cyber Europe*. ENISA. (2021, September 18). Retrieved June 26, 2022, from https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

[24] Henderson, C. (2019, November 7). *Most hackers aren't criminals*. The New York Times. Retrieved June 26, 2022, from https://www.nytimes.com/2019/11/07/opinion/hackers-hacking.html.

[25] *How can countries respond to and deter cyber attacks? - AEI*. (n.d.). Retrieved June 26, 2022, from https://www.aei.org/foreign-and-defense-policy/how-can-countries-respond-to-and-deter-cyber-attacks/.

[26] *Cyberterrorism*. CEPOL. (2018, November 6). Retrieved June 26, 2022, from https://www.cepol.europa.eu/tags/cyberterrorism.

[27] Wigan Council. (n.d.). Cyber terrorism. Retrieved June 26, 2022, from https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx.

[28] *Use of the internet*. United Nations : Office on Drugs and Crime. (n.d.). Retrieved June 26, 2022, from https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html.

[29] *What is a VPN? virtual private network meaning*. NordVPN. (2022, June 23). Retrieved June 26, 2022, from https://nordvpn.com/what-is-a-vpn/.

monitor, or otherwise control the activities of VPN users."[30] When people access VPNs, their location, personal information, and digital footprint on the cybersphere is severely blurred out or wiped completely, leading to a loss of control over online movement from the government in their country.

Deindividuation Theory

Deindividuation theory, a philosophical idea explored over thousands of years, is the view that people will engage in "impulsive, deviant, and sometimes violent acts in situations in which they believe they cannot be personally identified."[31] This idea, when applied to the Internet, can lead to cyberbullying and other forms of online harassment or even criminal behavior that can escalate because "individuals feel that they can no longer be identified as individuals but instead are…the larger group."[32] Screens act as a medium for global communication, but simultaneously take away the tangible experience of conversing and interacting with others in person. Thus, delegates should consider ways that deindividuation theory applies to cybercrime and how the phenomenon may "liberat[e] individuals to commit software piracy"[33] in order to understand potential factors behind digital attacks.

Universal Declaration of Human Rights (UDHR)

The Universal Declaration of Human Rights, a "common standard of achievement" meant to"spell out basic civil, political, economic, social, and cultural rights,"[34] was first adopted by the General Assembly in 1948. The ratification of this international treaty denotes the obligation in which Member States must protect individuals and groups from the abuse of human rights and refrain from the enjoyment of liberties through all means necessary. In late 2016, this piece of legislation was further developed to include "[t]he promotion, protection, and enjoyment of human rights on the Internet."[35] This addition was motivated by the UN Sustainable Development Goals' aim to create partnerships between countries.With this in mind, the protection and promotion of basic Internet services could be a prime factor in setting up a road to a united international cyberspace in the future.

International Telecommunications Union (ITU)

[30] *Are vpns legal? 10 countries that ban the usage of VPN*. WHSR. (2022, March 30). Retrieved June 26, 2022, from https://www.webhostingsecretrevealed.net/blog/security/are-vpns-legal/.

[31] Encyclopædia Britannica, inc. (n.d.). *Deindividuation*. Encyclopædia Britannica. Retrieved June 26, 2022, from https://www.britannica.com/topic/deindividuation.

[32] Birch, E. S. (2010). *Deindividuation in the online social networking context: What situations might encourage deindividuation on Facebook?* Retrieved June 27, 2022, from https://mro.massey.ac.nz/bitstream/handle/10179/3225/02_whole.pdf?sequence=1.

[33] S;, H. (n.d.). *Deindividuation and internet software piracy*. Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society. Retrieved June 27, 2022, from https://pubmed.ncbi.nlm.nih.gov/18721086/.

[34] United Nations. (n.d.). *International human rights law*. OHCHR. Retrieved June 27, 2022, from https://www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law.

[35] Howell, C., & West, D. M. (2022, March 9). *The internet as a human right*. Brookings. Retrieved June 27, 2022, from https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/.

Every time someone on Earth uses a mobile phone, accesses the Internet, or sends a digital email, they do so based on the work of the International Telecommunications Union (ITU). As a wing of the United Nations, the union involves all 193 Member States to “facilitate international connectivity in communications networks” while the union also “develops the technical standards that ensure networks and technologies seamlessly interconnect” while striv[ing] to improve access to ICTs to underserved communities worldwide.”[36] In recent years, and with the coronavirus pandemic shutting down thousands of schools and other public institutions, the organization has turned their attention to the accessibility of technology for all regardless of socioeconomic status. The ITU Secretary-General Houlin Zhao commented: “[e]quitable access to digital technologies isn’t just a moral responsibility, it’s essential for global prosperity and sustainability”[37]—however, certain legislations passed by the organization have been controversial. In 2012, 89 Member States passed a resolution that allowed for “all governments [to] have an equal role and responsibility for international Internet governance.” The head of the U.S. delegation at the time, Terry Kramer, cited the reason behind the U.S. not signing the treaty: “[t]he US has consistently believed and continues to believe that the (UN treaty) should not extend to Internet governance or content.”[38] Seeing as cyberspace is a relatively new environment, the entire world is facing a dilemma on which humanitarian rights digital users are entitled to, and how to enforce them across or within borders.

Global Cybersecurity Agenda (GCA)

According to the International Telecommunications Union, the 2007 Global Cybersecurity Agenda is “a framework for international cooperation aimed at enhancing confidence and security in the information society.”[39] This objective manifests in ways such as but not limited to “developing National Computer Incident Response Teams (CIRTs), cultivating cyber tactics as a national resource,” and “educating citizens and raising awareness of cybersecurity problems.”[40] The agenda also stresses the importance of “all countries arriv[ing] at a common understanding regarding cybersecurity” alongside]“a framework for international cooperation”[41]—a theme that may be increasingly difficult to come to fruition as countries face larger socio-political divides over future applications of cyberspace.

[36] United Nations. (n.d.). *About the International Telecommunication Union (ITU)*. ITU. Retrieved June 27, 2022, from https://www.itu.int/en/about/Pages/default.aspx.

[37] Price, G. (2022, June 6). *New Data, statistics: ITU releases 2022 Global Connectivity Report, global potential of internet remains largely untapped*. Library Journal infoDOCKET. Retrieved June 27, 2022, from https://www.infodocket.com/2022/06/06/itu-releases-2022-global-connectivity-report-global-potential-of-internet-remains-largely-untapped/.

[38] Khalil, A. (2012, December 14). *89 nations sign the controversial UN Telecom Treaty*. Phys.org. Retrieved June 27, 2022, from https://phys.org/news/2012-12-nations-controversial-telecom-treaty.html.

[39] *Global cybersecurity agenda (GCA)*. ITU. (n.d.). Retrieved June 27, 2022, from https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

[40] United Nations. (n.d.). *Global cybersecurity agenda (GCA) - United Nations office on drugs and ...* International Telecommunications Union. Retrieved June 27, 2022, from https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf.

[41] *Global cybersecurity agenda*. f3magazine.unicri.it. (2014, March 19). Retrieved June 27, 2022, from https://f3magazine.unicri.it/?p=350.

Timeline of Key Events

1971 - The World's First Computer Virus "The Creeper System"

In 1969, an experimental computer network dubbed 'ARPANET' was created to "computer to computer over long distances, without the need for a dedicated phone connection between each computer."[42] Known as the precursor to the Internet, the program was mostly used by experimental scientists looking to further develop the cybersphere.In 1971, though, all connected teletype computer screens displayed the message: 'I'm the creeper, catch me if you can!' However, this particular phenomenon was revealed to not be created with malicious intent, but instead by researcher Bob Thomas in order to "test self-duplicating program[s]...to illustrate a mobile application."[43] The virus displayed the taunting challenge to scientists eager to explore new possibilities and invent in response to digital problems. Bob's objective did not disappoint, as the Creeper led to the birth of the world's first antivirus program in response—the Reaper[44]. This creation would mark the start of thousands of new cybersecurity programs, for businesses, schools, hospitals, and entire nations, to come.

1976 - 2006 - The World's Largest Insider Attack

Over the span of thirty years, Boeing Company, an American aerospace manufacturing organization, suffered a loss of $2 billion worth of confidential documents to leaks by their employee Greg Chung. He was convicted for "acting as an agent of the People's Republic of China…for whom he stole restricted technology…[and] information related to the Space Shuttle program and the Delta IV rocket."[45] The implications of his attack were immense—according to then-U.S. Attorney Thomas P. O'Brien, Chung "compromised not only the American company that developed and owned the trade secrets, but national security as well…the secrets could be used by the PRC to develop its own military technology."[46] This was one of the largest historical insider attacks with malicious intentions to supply China with proprietary military and spacecraft intelligence—"not just a threat to Boeing, but to the entire [United States] as well."[47]

[42] Matthews, T. (2022, February 16). *Creeper: The World's first computer virus*. Exabeam. Retrieved June 28, 2022, from https://www.exabeam.com/information-security/creeper-computer-virus/.

[43] Techopedia. (2011, August 18). *What is a creeper virus? - definition from Techopedia*. Techopedia.com. Retrieved June 28, 2022, from https://www.techopedia.com/definition/24180/creeper-virus.

[44] *The creeper and the reaper make cybersecurity history*. Smarter MSP. (2020, October 16). Retrieved June 28, 2022, from https://smartermsp.com/the-creeper-and-the-reaper-make-cybersecurity-history/.

[45] *Former Boeing engineer convicted of economic espionage in theft of Space Shuttle Secrets for China*. The United States Department of Justice. (2014, September 16). Retrieved June 28, 2022, from https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china.

[46] *Former Boeing engineer convicted of economic espionage in theft of Space Shuttle Secrets for China*. The United States Department of Justice. (2014, September 16). Retrieved June 28, 2022, from https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china.

[47] Sarah Hospelhorn Based in Brooklyn, Hospelhorn, S., Brooklyn, B. in, Sobers, R., & By. (n.d.). *8 events that changed cybersecurity forever*. Varonis. Retrieved June 28, 2022, from https://www.varonis.com/blog/events-that-changed-cybersecurity.

November 2, 1988 - May 5, 1990 - The Morris Worm

A year before the invention of the World Wide Web, a malicious program released from the Massachusetts Institute of Technology "infected systems at a number of prestigious colleges and public and private research centers that made up the early national electronic network…[a]mong the many casualties were Harvard, Princeton, Stanford, Johns Hopkins, NASA, and the Lawrence Livermore National Laboratory"[48]. The program eventually was beat after "twelve hours…[a] team at Berkeley came up with steps that would help [prevent] the spread of the virus…[and a]nother method was also discovered at Purdue and widely published"[49]. However, at that point, the damage was done – the U.S Government Accountability Office put the estimated cost of repairs for each installation of the worm from $100,000 to $10,000,000. Its origin was traced back to a 23-year-old student at Cornell University, Robert Morris, who meant for his worm to expose how quickly an attack could unfold, but…made a devastating coding mistake"[50]. Morris avoided jail time but received a hefty fine and a probational sentence.

November 23, 2001 - The Budapest Convention on Cybercrime Is Passed

The Council of Europe was the world's first organization to adopt a international treaty addressing cybercrime by "harmonizing national laws, improving investigative techniques, and increasing cooperation among nations"[51] in 2001. Some of the key aspects of the legislation include "mandat[ing]...the adoption of legislation that outlaw[s] specified cyber related crimes" and "requir[ing]…certain evidence-gathering rules, such as mechanisms to support…the expedited preservation of stored data."[52] Although 65 Member States have entered into the agreement, delegations such as India and Brazil have refused to adopt the convention, reasoning that their absence during its initial creation prevents them from doing so.[53] Russia also opposes the treaty, but instead on different grounds – adoption would "violate principles of state sovereignty" and "allow[s] cross-border cybercrime operations". This prompted a series of criticism around the world, including that of The Lowy Institute, who argued that "[it's] hard to see how Russia could engage in negotiations for a legally-binding cybercrime treaty in good faith"[54]. In recent years, India has brought up reconsidering their stance on not

[48] FBI. (2018, November 2). *The Morris worm*. FBI. Retrieved June 29, 2022, from https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

[49] Kehoe, B. P. (n.d.). *The Robert Morris Internet Worm*. Research. Retrieved June 29, 2022, from https://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html.

[50] *What is the Morris Worm? history and modern impact*. Okta. (n.d.). Retrieved June 29, 2022, from https://www.okta.com/identity-101/morris-worm/#:~:text=The%20Morris%20worm%20was%20created,a%20bit%20of%20a%20prankster.

[51] *The Budapest Convention on Cybercrime: A Framework for Capacity Building*. Global Forum on Cyber Expertise. (n.d.). Retrieved June 30, 2022, from https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/.

[52] *Budapest convention: What is it and how is it being updated?: Cross-border Data Forum*. Cross. (2022, June 7). Retrieved June 30, 2022, from https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

[53] Council of Europe. (n.d.). *The Budapest Convention on Cybercrime: Benefits and ... - council of Europe*. Retrieved June 30, 2022, from https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

[54] Page, M. (2022, March 7). *The hypocrisy of Russia's push for a new global cybercrime treaty*. The Interpreter. Retrieved June 30, 2022, from https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

joining after a surge in cybercrime, although their hesitation over sharing data with foreign delegations and agencies remain[55].

October 2012 - January 2013 - Operation Red October Is Uncovered

Operation Red October was a cyberespionage malware program that "targeted a range of diplomatic facilities, defense companies, and energy firms around the world" for nearly five years before being discovered by the Russian firm Kaspersky Lab in late 2012.[56] Kaspersky launched an investigation almost immediately afterwards, but to this day the attackers' true identities are still unknown. However, the search was not completely unsuccessful; it was uncovered that the attackers "often used information exfiltrated from infected networks as a way to gain entry into additional systems…[for example], stolen credentials were compiled in a list and used when the attackers needed to guess passwords or phrases."[57] This event led many experts to question whether or not countries could ever truly unite in cyberspace if "there could lurk unidentified dark forces…by Countries that are interested to steal information which they consider vital for their survival."[58] Unifying cyberspace means providing ways for the rest of the world to access personal information – and not everyone is willing to give such trust.

June 2013 - Edward Snowden Blows the Whistle

Edward Snowden is an American computer security consultant who, in mid-2013, leaked confidential information from the National Security Agency under which he was employed at the time. His acts revealed the existence of several illegal monitoring systems by the government onto American citizens, prompting a worldwide discussion about the influence of national powers on individual safety and security.[59] Snowden also made a number of allegations against the Government Communications Security Bureau of New Zealand, accusing them of unlawfully surveilling their people and committing acts of espionage.[60] In late 2020, a U.S. federal court ruled that in the case of *United States v. Moalin*, that the American government intelligence's mass surveillance program, exposed by Snowden, was illegal and

[55] Tripathi, R. (2018, January 17). *Home Ministry pitches for Budapest Convention on Cyber Security*. The Indian Express. Retrieved June 30, 2022, from https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/.

[56] Author(s) Maschenka Braganca. (n.d.). *Hunt for red October: The new face of cyber espionage*. Hunt for Red October: The New Face of Cyber Espionage | Office of Justice Programs. Retrieved July 1, 2022, from https://www.ojp.gov/ncjrs/virtual-library/abstracts/hunt-red-october-new-face-cyber-espionage.

[57] Kaspersky. (2021, May 26). *Kaspersky Lab identifies Operation "Red October," an advanced cyber-espionage campaign targeting diplomatic and government institutions worldwide*. www.kaspersky.com. Retrieved July 1, 2022, from https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide.

[58] Teti, A. (n.d.). *Operation 'red october': And it is Cyber Espionage*. GNOSIS. Retrieved July 2, 2022, from https://gnosis.aisi.gov.it/gnosis/Rivista34.nsf/ServNavigE/34-09.pdf/$File/34-09.pdf?OpenElement.

[59] Encyclopædia Britannica, inc. (n.d.). *Edward Snowden*. Encyclopædia Britannica. Retrieved July 2, 2022, from https://www.britannica.com/biography/Edward-Snowden.

[60] Greenwald, G., & Gallagher, R. (2014, September 15). *New Zealand launched Mass Surveillance Project while publicly denying it*. The Intercept. Retrieved July 2, 2022, from https://theintercept.com/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/.

unconstitutional.[61] The United States, alongside many other countries, were divided on whether or not Snowden was a patriotic hero or a national traitor—and many lost trust in their government, worried that their online presence could be used against them in some way.

June 27, 2018 - June 28, 2018 - Petya Ransomware Attack

One of the most powerful cyberattacks in digital history was the Petya ransom program that endangered ministries, electrical grids, newspapers, and banks in countries such as France, Germany, Russia, the United States, the United Kingdom, and Australia. However, according to the journalist platform Associated Press, experts agreed that Peyta was "masquerading as ransomware, while it was actually designed to cause maximum damage, with Ukraine being the main target."[62] Investigations did not lead to definite conclusions, but signs pointed to the virus originating from an infected update of a Ukrainian tax accounting system, named 'MeDoc,' developed by the company Intellect Service – although their representatives were quick to deny the allegations.[63] It is widely believed that the attack intended to cripple the Ukrainian state, ahe attack came on the eve of the Ukrainian public holiday, Constitution Day. Most government buildings, officers, and security businesses would be empty, which would give the cyberattack time to spread without being caught. Additionally, the ransomware reportedly wiped the affected hard drives rather than encrypting them for personal use, which would be a further disaster for companies that lose years of their work.[64] Petya's complete crippling of computers and devices in a multinational attack demonstrated to the world just how uncontrollable and damaging ransomware attacks could develop.

February 15, 2022 - Ukraine's Defense Ministry is Hacked

Russia's ongoing invasion of Ukraine involves trenches, tear gas, tanks – but their work had begun long beforehand, with a vast range of weaponized technologies. According to Ukraine's minister of digital transformation, Mykhailo Fedorov, February 15th's "vectors of attacks were organized from different countries…to destabilize, to sow panic, to create a certain chaos in the actions of Ukranians in our country." While an official confirmation on the perpetrator still has not been announced, nor have any nations or terrorist groups claimed credit for the attack since, Ilya Vityuk, the Head of the Ukrainian Intelligence Agency's Cyber Security Department, placed blame on Russia's government at the time. In

[61] Satter, R. (2020, September 2). *U.S. court: Mass surveillance program exposed by Snowden was illegal*. U.S. Retrieved July 2, 2022, from https://web.archive.org/web/20201101085850/https://www.reuters.com/article/us-usa-nsa-spying/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK.

[62] Bajak, F. (2017, June 30). *Companies still hobbled from fearsome cyberattack*. AP NEWS. Retrieved July 2, 2022, from https://apnews.com/article/russia-ukraine-technology-business-europe-hacking-ce7a8aca506742ab8e8873e7f9f229c2.

[63] Wakefield, J. (2017, June 28). *Tax software blamed for cyber-attack spread*. BBC News. Retrieved July 2, 2022, from https://www.bbc.com/news/technology-40428967.

[64] Kramer, A. E. (2017, June 28). *Ukraine cyberattack was meant to paralyze, not profit, evidence shows*. The New York Times. Retrieved July 2, 2022, from https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html.

his words, the only country that "...[was] interested in such strikes on our country, especially against the background of mass panic… [was] unfortunately, the Russian Federation."[65] Many experts believed that this cyberattack was an attempt to weaken Ukrainian defenses before Russian forces ultimately penetrated them.

Position of Key Member Nations and Other Bodies

United States of America

As one of the world's digital powerhouses, the United States is largely dependent on the Internet—and while this reliance may help power national security systems, optimize transportation, and more, it also exposes the country to external cyberspace threats.[66] In fact, it was found that between May 2006 and June 2020, the United States experienced 156 foreign strikes on their online security systems, the most significant number of cyberattacks in the entire international community during that time.[67] In that same vein, with nearly 800,000 victims of ransom and blackmail and an estimated 4.2 billion dollars in loss in 2020 alone[68], the United States has repeatedly condemned the spread in cybercrime and encourages all countries to cooperate in investigations to ensure right forms of justice given in response.[69] Furthermore, in recent years, the U.S. Homeland Security organization rolled out a multifaceted plan that addressed the need to fortify the cyber resistance of the nation's transportation, protect water treatment facilities and other vital resources, and created a national task force responsible for elevating the fight against ransomware.[70] American policy on the matter also extends internationally—on April 20, 2022, alongside Australia, Canada, New Zealand, and the United Kingdom, a joint Cybersecurity Advisory (CSA) was formed in order to express concerns that the Russian government was exploring options for future cyberattacks and other malicious activity in response to the economic sanctions placed on it as a result of their current invasion of Ukraine (2022-ongoing).[71]

Russian Federation

[65] Hopkins, V. (2022, February 15). *A hack of the Defense Ministry, Army and State Banks was the largest of its kind in Ukraine's history.* The New York Times. Retrieved June 29, 2022, from https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html.

[66] Pomerleau, M. (2021, August 16). *Who can match the US as a cyber superpower? no one*. C4ISRNet. Retrieved July 6, 2022, from https://www.c4isrnet.com/cyber/2021/06/28/who-can-match-the-us-as-a-cyber-superpower-no-one/.

[67] Ravacon, A. (2020, July 13). *The countries experiencing the most 'significant' cyber-attacks*. Specops Software. Retrieved July 6, 2022, from https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/.

[68] *Cybercrime victims lose an estimated $318 billion annually*. Comparitech. (2022, February 3). Retrieved July 6, 2022, from https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/.

[69] FBI. (2001, June 12). *The FBI's perspective on the cybercrime problem*. FBI. Retrieved July 6, 2022, from https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem.

[70] *Cybersecurity*. Cybersecurity | Homeland Security. (n.d.). Retrieved July 6, 2022, from https://www.dhs.gov/topics/cybersecurity.

[71] *Alert (AA22-110A)*. CISA. (n.d.). Retrieved July 6, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Over the years, the Russian Federation has gained the infamous reputation of being one of the world's leading 'cybercrime citadels,' as both their government and citizens have been repeatedly accused of launching attacks against other nations and peoples around the world. Breaching confidential data, committing espionage, and rigging elections are just a few of the list of crimes that have been traced back to Russian hackers[72]. Furthermore, in 2021, an analysis cited by the BBC suggested that nearly 74% of all money made through international ransomware attacks went to groups "highly likely to be affiliated with Russia", despite the fact that the country had for years been denying that their government facilitated, encouraged, or harbored cybercriminals in any shape or form[73]. Max Goncharov, a threat researcher at the security firm Trend Micro, noted that "[Russian] barriers to underground market entry [are] lower than ever…anyone who's interested in launching a cybercrime business can find partners and required tools online"[74]—a result that worries many countries around the world, as warfare programs shift online. As of 2022, Russia is most closely allied with Belarus, China, Kazakhstan, Armenia, and India, while their adversaries include nations such as the United States, Ukraine, the United Kingdom, Poland, and Lithuania[75].

Japan

Despite being a nation leading in technological developments, Japan has been criticized for its 'breeding ground' of cybercrime and are urged to put more efforts towards fortifying their defenses against online attacks. In fact, according to the IT company Eire Systems, cybercrime "thrives in the shadows…and Japanese society creates those shadows by not acknowledging this new type of hidden antisocial behavior", putting the cause of rampant national cybercrime behind a lack of deliberate action rather than a lack of the resources needed to protect Japan's cybersphere[76]. In the past, Japanese companies and government agencies employed 'passive' defense tactics that focused on rapid recovery after an attack, but in recent years, more people in the country have brought idea of shifting to a defense that actively seeks out and destroys threats before they occur[77]. Washington and Japan strengthened their

[72] *The Dark Side of Russia: How New Internet laws and Nationalism fuel Russian cybercrime*. IntSights, a Rapid7 Company - Cyber Threat Intelligence. (n.d.). Retrieved July 7, 2022, from https://intsights.com/resources/how-new-internet-laws-and-nationalism-fuel-russian-cybercrime.

[73] Tidy, J. (2022, February 14). *74% of ransomware revenue goes to Russia-linked hackers*. BBC News. Retrieved July 7, 2022, from https://www.bbc.com/news/technology-60378009.

[74] Schwartz, M. J., & Ross, R. (n.d.). *Why Russian cybercrime markets are thriving*. Bank Information Security. Retrieved July 7, 2022, from https://www.bankinfosecurity.com/russian-cybercrime-markets-are-thriving-a-8439.

[75] Buchholz, K., & Richter, F. (2022, February 18). *Infographic: Russia's friends and foes*. Statista Infographics. Retrieved July 7, 2022, from https://www.statista.com/chart/26876/russias-friends-and-foes-survey/.

[76] *Why Japan should implement a cyber security strategy*. EIRE Systems. (2021, December 1). Retrieved July 8, 2022, from https://www.eiresystems.com/why-japan-needs-to-step-up-its-cyber-security-game/.

[77] Lewis, L. (2021, September 11). *Japan is belatedly recognising the risks of Cyber War* . Subscribe to read | Financial Times. Retrieved July 10, 2022, from https://www.ft.com/content/43f7cc53-3ed5-4df9-92fd-3823e36a8f05.

cooperation and support on cybercrime with one another in 2019, in order to "ensure the Alliance's superiority in a contingency and to safeguard institutions and rules-based order during peacetime"[78].

People's Republic of China

The two most vital organizations that handle Internet related crimes in China are the Public Security Bureau, which protects internal national security, and the Ministry State Security, responsible for monitoring external threats to Chinese cyberspace[79]. As the collective Law Enforcement Authority, the organizations work together to processes thousands of requests for investigation assistance and incoming information from Interpol, and have established law enforcement cooperation networks with more than 70 countries and regions[80]. Despite this, China had approximately 62,000 cases of cybercrime reported in 2021 alone, all of which ranged from offenses such as infringement of intellectual property, online gambling, fraud, and the manufacturing of fake goods[81].

One of the most controversial of China's cyber crimes was linked to the country's persecution of the Uyghur Muslim community, in which it was found that Chinese hackers "posed as journalists, students, human rights advocates or members of the Uyghur community [in order] to build trust with people they targeted and trick them into clicking on malicious links"[82]. The FBI investigation further established that China used the cybersphere to reach out to journalists who were attacking the country over allegations of unlawful Uyghur imprisonments, to discourage, intimidate, and silence the spread of these critiques. The United States warned the Chinese government to cease "transnational repression activity [that] violates US laws and individual rights", while the latter continues to firmly deny any digital wrongdoings[83].

United Kingdom

In 2021 alone, the United Kingdom (composed of the states Wales, England, Northern Ireland, and Scotland) reported over 400,000 cases of fraud and cybercrime that cost nearly 3.1 billion pounds to repair[84]. Experts are speculating that economic loss caused by the ongoing pandemic may have caused

[78] Hurst, D. (2019, April 26). *Japan, US beef up their cyber alliance*. – The Diplomat. Retrieved July 10, 2022, from https://thediplomat.com/2019/04/japan-us-beef-up-their-cyber-alliance/.

[79] *Cybercrime Laws People's Republic of China*. CyberCrime Law. (n.d.). Retrieved July 10, 2022, from https://www.cybercrimelaw.net/China.html.

[80] UNODC. (n.d.). *Comments on China*. UNODC. Retrieved July 10, 2022, from https://www.unodc.org/documents/Cybercrime/English.pdf.

[81] 秦琪. (n.d.). *China handles 62,000 cybercrime cases in 2021*. The State Council Information Office of the People's Republic of China. Retrieved July 10, 2022, from http://english.scio.gov.cn/pressroom/2022-01/06/content_77972842.htm.

[82] O'Sullivan, D. (2021, March 26). *Chinese hackers targeted Uyghurs living in us, Facebook Security Team finds*. CNN. Retrieved July 18, 2022, from https://edition.cnn.com/2021/03/24/tech/uyghurs-hacking/index.html.

[83] Page, C. (2021, September 2). *FBI says Chinese authorities are hacking US-based Uyghurs*. TechCrunch. Retrieved July 18, 2022, from https://techcrunch.com/2021/09/02/fbi-china-hacking-uyghurs/.

[84] O'Driscoll, A. (2022, May 18). *UK cyber security and Cyber Crime Statistics in 2022*. Comparitech. Retrieved July 18, 2022, from https://www.comparitech.com/blog/information-security/uk-cyber-security-statistics/#:~:text=There%20were%20over%20400%2C000%20reports,individuals%20and%2060%2C111%20from%20businesses..

hackers to target larger businesses, corporations, organizations, which make up nearly 4,000 of cyber crime victims from September 2019 to September 2020[85]. The UK's current Computer Misuse Act, a piece of legislation that has long been criticized for its ineffectiveness, carries several loopholes that expose the UK's economy and critical infrastructure to criminals on the cybersphere[86]. In response, establishments such as Google, Microsoft, and the University of Cambridge have been working to create new hardware and software programs that better secure private information for users across the country. In 2019, their academic prototypes were awarded with 70 million pounds from the UK government, which enabled Cambridge researchers—alongside the University of Edinburgh—to create "a ground-breaking and unprecedented industrial-scale prototype…in the context of architecture"[87]. Leaders are calling for a stronger focus on computer sciences and development in the future in order to fortify their cybersphere.

Republic of India

The rise in digital currency has provided the Delhi Police's Cyber Crime Unit with a new obstacle—cryptocurrency systems are quickly becoming a means for illegal transactions, blackmail, theft, and more[88]. Over the past two years, financial cybercrime in India has become increasingly common, resulting in individuals suffering huge economic losses and severe violations of confidential data and privacy[89]. But it's not just the single citizen who's at threat—at a national cyber security conference in mid-2022, Union Home Minister Amit Shah stated that the entire country was under threat by 'cyber armies' ready to launch attacks (although later he reassured that the government was doing all they could to protect citizens)[90]. In response, researchers urge two essential plans of action; firstly conducting more analysis on India's cybersphere would make up for the lack of concrete data that has so far been preventing a detailed study of financial cyber-fraud. Secondly, regulator organizations such as the Reserve Bank of India must "evolve their safety features and security processes of all stakeholders in the digital

[85] Security Magazine. (2020, October 23). *UK sees a 31% increase in cyber crime amid the pandemic*. Security Magazine RSS. Retrieved July 18, 2022, from https://www.securitymagazine.com/articles/93722-uk-sees-a-31-increase-in-cyber-crime-amid-the-pandemic.

[86] Guardian News and Media. (2020, January 22). *Cybercrime laws need urgent reform to protect UK, says report*. The Guardian. Retrieved July 18, 2022, from https://www.theguardian.com/technology/2020/jan/22/cybercrime-laws-need-urgent-reform-to-protect-uk-says-report.

[87] Fell, S. (2022, May 25). *Making the Digital World A Safer Place*. University of Cambridge. Retrieved July 18, 2022, from https://www.cam.ac.uk/stories/improving-computer-security.

[88] Sinha, J. (2022, July 18). *New Challenge for Delhi Cyber Unit: Crypto*. The Indian Express. Retrieved July 18, 2022, from https://indianexpress.com/article/cities/delhi/new-challenge-for-delhi-cyber-unit-crypto-8035547/.

[89] Saha, B. S. (2022, July 14). *OTP, KYC, pin theft biggest reasons for phishing and cybercrime in India*. MediaNama. Retrieved July 18, 2022, from https://www.medianama.com/2022/07/223-dialogue-report-phishing-cybercrime-fraud-india/.

[90] Correspondent, S. (2022, June 20). *Forces inimical to India have 'cyber armies' to launch cyberattacks against India: Home minister Amit Shah*. Return to frontpage. Retrieved July 18, 2022, from https://www.thehindu.com/news/national/forces-inimical-to-india-have-cyber-armies-to-launch-cyberattacks-against-india-home-minister-amit-shah/article65545112.ece.

payments ecosystem for greater harmonization and user safety…noting that this will also help law enforcement agencies to investigate crimes”[91].

Sweden

Although Sweden is one of the world's most well-connected countries, with nearly 93% of their population having access to the Internet, it is also one of the safest of national cyber spheres. The Swedish government has placed no restrictions on how citizens access the Internet besides those around the infringement of personal rights, and there have not been any substantial reports that emails and texts of Swedish citizens have been monitored or recorded in any way without proper judicial authorization[92]. However, amongst the few cases of attacks, almost 20% of them occur in the manufacturing industry, leading to a growing demand for intrusion prevention systems, anti-virus software, biometric technology, wireless and applications security solutions, and more[93]. In the future, Sweden plans to apply new technologies such as AI and IoT to solve larger societal challenges, while [simultaneously] retaining values such as openness, collaboration, integrity and ethics”[94].

Suggested Solutions

The first solution that must be taken in order to ensure peace in cyberspace is to reduce the gap in cybersecurity skills to ensure the personal protection of valuable belongings and information. By “creating a sustainable pipeline of cybersecurity talent”, countries can better fine-tune their action against cybercrime with the help and greater participation of digital professionals. As of early 2022, the cybersecurity workforce gap includes nearly 2.72 million positions, and according to the 2021 ISC Cybersecurity Workforce Study, the industry needs to expand 65% more in order to properly defend organizations' assets.[95] But experts predict that no sole organization can make the changes necessary on their own—this is a responsibility that must be taken on through partnerships between industries, academia, governments and leaders, and more. Steps such as investing in cyber lessons at school and the sector as a whole, recognizing online security as a core element in the workplace, hiring experts with a combination of technology experience and mentoring expertise, and enhancing a nation's understanding

[91] Saha, B. S. (2022, July 14). *OTP, KYC, pin theft biggest reasons for phishing and cybercrime in India*. MediaNama. Retrieved July 18, 2022, from https://www.medianama.com/2022/07/223-dialogue-report-phishing-cybercrime-fraud-india/.

[92] Johnny 5 on January 5, (2021, October 4). *ExpressVPN: Online privacy is why Sweden wins the internet*. Home of internet privacy. Retrieved July 18, 2022, from https://www.expressvpn.com/blog/online-privacy-is-why-sweden-wins-the-internet/#:~:text=The%20Swedish%20government%20places%20no,monitored%20without%20proper%20judicial%20authorization..

[93] 7. (n.d.). *Sweden - cyber security opportunities*. International Trade Administration | Trade.gov. Retrieved July 18, 2022, from https://www.trade.gov/market-intelligence/sweden-cyber-security-opportunities.

[94] *Sweden's digital technologies ecosystem*. Sweden's Digital Technologies Ecosystem - Business Sweden. (n.d.). Retrieved July 18, 2022, from https://www.business-sweden.com/markets/sweden/swedens-digital-technologies-ecosystem/.

[95] *Can closing the cybersecurity skills gap change the world?* World Economic Forum. (n.d.). Retrieved July 19, 2022, from https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap/.

of the cybersphere through continuous and long-term studies, are all components of improving digital security skills[96].

A second possible solution could lie in international teamwork; encouraging all member States to formulate and implement a national cyber security or cyber defense strategy would help identify cyber threats, mitigation systems, and how to properly defend personal information in the case of an attack[97]. Cybercrime Magazine was able to highlight just how extreme and widespread the threat to cyber peace is: "if it were measured as a country, then cybercrime—which is predicted to inflict damages totaling $6 trillion USD globally in 2021—would be the world's third-largest economy after the U.S. and China".[98] Despite this alarming statistic, 13% of all countries in the world have no cyber crime laws whatsoever, and the ones that do, often possess loopholes or are severely outdated and don't accommodate new developments in technology.[99] The International Telecommunication Union, a communication agency of the United Nations, recommends that all governments include objectives in their legislation such as but not limited to "legal frameworks, early warning and response mechanisms, capacity building and training, research and development, and international collaboration".[100]

Finally, the third solution would encourage higher transparency and accountability for governments that use technology in order to ensure that citizens understand their rights to privacy and not be unlawfully monitored online.[101] This could be achieved through constant supervision of certified, legal organizations outside of a national government (or government-affiliated organization) to ensure ethical conductivity and prevent the abuse of power during investigations that involve online movements. Additionally, nations with people protesting reports of government misconduct with the civilian cybersphere should be heavily encouraged to tighten regulations, such as those that involve bugging, wiretapping, and any other form of invasive surveillance. This could ensure that the Internet becomes a tool used lawfully and recognized to be for the greater good of a community or nation rather than a threat to personal privacy and safety.

Although the world is well-versed in handling crimes in real life, those in the digital world are still mysterious and leave room for a lot more exploration to fully understand. Despite this, they are still

[96] *Here's why closing the skills gap is key to digitalization*. World Economic Forum. (n.d.). Retrieved July 19, 2022, from https://www.weforum.org/agenda/2021/11/heres-why-closing-skills-gap-key-to-digitalization/.

[97] *National strategies*. ITU. (n.d.). Retrieved July 19, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

[98] Cybercrimemag. (2021, April 27). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. Retrieved July 19, 2022, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

[99] *Cybercrime legislation worldwide*. UNCTAD. (n.d.). Retrieved July 19, 2022, from https://unctad.org/page/cybercrime-legislation-worldwide.

[100] *ITU-D Cybersecurity*. ITU Development Cybersecurity. (n.d.). Retrieved July 19, 2022, from https://www.itu.int/itu-d/sites/cybersecurity/.

[101] Kuner, Christopher. "International Data Privacy Law." *Academic.oup.com*, Oxford Academic, Feb. 2022, https://academic.oup.com/idpl.

becoming increasingly common as scientists develop new technologies and the Internet encompasses almost every aspect of urban activity. When the Internet and other forms of online media are available to millions of people around the world, steps to achieve peace in this cybersphere and prevent conflict are crucial. Action must be congruent with measures to protect the privacy of citizens while simultaneously dealing with future digital crimes must be implemented in the long run to prevent a new host of warfare, attacks, ransom, blackmail, and other notorious crimes—online.

Bibliography

7 social media sites and their data breaches. humanID. (2022, June 21). Retrieved June 23, 2022, from https://human-id.org/blog/biggest_social_media_breach_history/.

7. (n.d.). *Sweden - cyber security opportunities*. International Trade Administration | Trade.gov. Retrieved July 18, 2022, from https://www.trade.gov/market-intelligence/sweden-cyber-security-opportunities.

Alert (AA22-110A). CISA. (n.d.). Retrieved July 6, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa22-110a.

Are vpns legal? 10 countries that ban the usage of VPN. WHSR. (2022, March 30). Retrieved June 26, 2022, from https://www.webhostingsecretrevealed.net/blog/security/are-vpns-legal/.

Author(s) Maschenka Braganca. (n.d.). *Hunt for red October: The new face of cyber espionage*. Hunt for Red October: The New Face of Cyber Espionage | Office of Justice Programs. Retrieved July 1, 2022, from https://www.ojp.gov/ncjrs/virtual-library/abstracts/hunt-red-october-new-face-cyber-espionage.

Birch, E. S. (2010). *Deindividuation in the online social networking context: What situations might encourage deindividuation on Facebook?* Retrieved June 27, 2022, from https://mro.massey.ac.nz/bitstream/handle/10179/3225/02_whole.pdf?sequence=1.

Buchholz, K., & Richter, F. (2022, February 18). *Infographic: Russia's friends and foes*. Statista Infographics. Retrieved July 7, 2022, from https://www.statista.com/chart/26876/russias-friends-and-foes-survey/.

The Budapest Convention on Cybercrime: A Framework for Capacity Building. Global Forum on Cyber Expertise. (n.d.). Retrieved June 30, 2022, from https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/.

Budapest convention: What is it and how is it being updated?: Cross-border Data Forum. Cross. (2022, June 7). Retrieved June 30, 2022, from https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

Can closing the cybersecurity skills gap change the world? World Economic Forum. (n.d.). Retrieved July 19, 2022, from https://www.weforum.org/agenda/2022/03/closing-the-cybersecurity-skills-gap/.

Correspondent, S. (2022, June 20). *Forces inimical to India have 'cyber armies' to launch cyberattacks against India: Home minister Amit Shah*. Return to frontpage. Retrieved July 18, 2022, from https://www.thehindu.com/news/national/forces-inimical-to-india-have-cyber-armies-to-launch-cyberattacks-against-india-home-minister-amit-shah/article65545112.ece.

Council of Europe. (n.d.). *The Budapest Convention on Cybercrime: Benefits and ... - council of Europe*. Retrieved June 30, 2022, from https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac.

The creeper and the reaper make cybersecurity history. Smarter MSP. (2020, October 16). Retrieved June 28, 2022, from https://smartermsp.com/the-creeper-and-the-reaper-make-cybersecurity-history/.

Cyber CEO: The History of Cybercrime, from 1834 to present. Herjavec Group. (2021, September 14). Retrieved June 23, 2022, from https://www.herjavecgroup.com/history-of-cybercrime/#:~:text=1834%20%E2%80%94%20French%20Telegraph%20System%20%E2%80%94%20A,conducting%20the%20world's%20first%20cyberattack.

Cyber Europe. ENISA. (2021, September 18). Retrieved June 26, 2022, from https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

Cybercrime Laws People's Republic of China. CyberCrime Law. (n.d.). Retrieved July 10, 2022, from https://www.cybercrimelaw.net/China.html.

Cybercrime legislation worldwide. UNCTAD. (n.d.). Retrieved July 19, 2022, from https://unctad.org/page/cybercrime-legislation-worldwide.

Cybercrime victims lose an estimated $318 billion annually. Comparitech. (2022, February 3). Retrieved July 6, 2022, from https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/.

Cybercrimemag. (2021, April 27). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. Retrieved July 19, 2022, from https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/.

Cybersecurity. Cybersecurity | Homeland Security. (n.d.). Retrieved July 6, 2022, from https://www.dhs.gov/topics/cybersecurity.

Cybersecurity. Cybersecurity | Ready.gov. (n.d.). Retrieved June 26, 2022, from https://www.ready.gov/cybersecurity.

Cyberterrorism. CEPOL. (2018, November 6). Retrieved June 26, 2022, from https://www.cepol.europa.eu/tags/cyberterrorism.

The Dark Side of Russia: How New Internet laws and Nationalism fuel Russian cybercrime. IntSights, a Rapid7 Company - Cyber Threat Intelligence. (n.d.). Retrieved July 7, 2022, from https://intsights.com/resources/how-new-internet-laws-and-nationalism-fuel-russian-cybercrime.

Doukidis, G., Mylonopoulos, N., Pouloudi, N., & Shepherd, J. (2004, January). *What is the Digital Era?* ResearchGate. Retrieved June 21, 2022, from https://www.researchgate.net/publication/344307301_What_is_the_Digital_Era.

Editor, C. S. R. C. C. (n.d.). *Cyberspace - glossary*. CSRC. Retrieved June 26, 2022, from https://csrc.nist.gov/glossary/term/cyberspace.

Encyclopædia Britannica, inc. (n.d.). *Cyberspace*. Encyclopædia Britannica. Retrieved June 26, 2022, from https://www.britannica.com/topic/cyberspace.

Encyclopædia Britannica, inc. (n.d.). *Deindividuation*. Encyclopædia Britannica. Retrieved June 26, 2022, from https://www.britannica.com/topic/deindividuation.

Encyclopædia Britannica, inc. (n.d.). *Edward Snowden*. Encyclopædia Britannica. Retrieved July 2, 2022, from https://www.britannica.com/biography/Edward-Snowden.

Encyclopædia Britannica, inc. (n.d.). *Stuxnet*. Encyclopædia Britannica. Retrieved June 24, 2022, from https://www.britannica.com/technology/Stuxnet.

FBI. (2001, June 12). *The FBI's perspective on the cybercrime problem*. FBI. Retrieved July 6, 2022, from https://archives.fbi.gov/archives/news/testimony/the-fbis-perspective-on-the-cybercrime-problem.

FBI. (2018, November 2). *The morris worm*. FBI. Retrieved June 29, 2022, from https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

Fell, S. (2022, May 25). *Making the Digital World A Safer Place*. University of Cambridge. Retrieved July 18, 2022, from https://www.cam.ac.uk/stories/improving-computer-security.

“'Extreme Surveillance' Becomes UK Law with Barely a Whimper.” *The Guardian*, Guardian News and Media, 19 Nov. 2016, https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper.

Fighting terror in cyberspace. World Scientific. (n.d.). Retrieved June 22, 2022, from https://www.worldscientific.com/worldscibooks/10.1142/5934.

The final report on nobelium's unprecedented nation-state attack. NTSC. (n.d.). Retrieved June 23, 2022, from https://www.ntsc.org/underwriters/underwriter-blogs/the-final-report-on-nobeliums-unprecidented-nation-state-attack.html.

Former Boeing engineer convicted of economic espionage in the theft of Space Shuttle Secrets for China. The United States Department of Justice. (2014, September 16). Retrieved June 28, 2022, from https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china.

Former Boeing engineer convicted of economic espionage in the theft of Space Shuttle Secrets for China. The United States Department of Justice. (2014, September 16). Retrieved June 28, 2022, from https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china.

Global cybersecurity agenda (GCA). ITU. (n.d.). Retrieved June 27, 2022, from https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

Global cybersecurity agenda. f3magazine.unicri.it. (2014, March 19). Retrieved June 27, 2022, from https://f3magazine.unicri.it/?p=350/

Greenwald, G., & Gallagher, R. (2014, September 15). *New Zealand launched Mass Surveillance Project while publicly denying it*. The Intercept. Retrieved July 2, 2022, from https://theintercept.com/2014/09/15/new-zealand-gcsb-speargun-mass-surveillance/.

Guardian News and Media. (2020, January 22). *Cybercrime laws need urgent reform to protect UK, says report*. The Guardian. Retrieved July 18, 2022, from https://www.theguardian.com/technology/2020/jan/22/cybercrime-laws-need-urgent-reform-to-protect-uk-says-report.

Henderson, C. (2019, November 7). *Most hackers aren't criminals*. The New York Times. Retrieved June 26, 2022, from https://www.nytimes.com/2019/11/07/opinion/hackers-hacking.html.

Here's why closing the skills gap is key to digitalization. World Economic Forum. (n.d.). Retrieved July 19, 2022, from https://www.weforum.org/agenda/2021/11/heres-why-closing-skills-gap-key-to-digitalization/.

The history of cybercrime: A comprehensive guide(2021). Jigsaw Academy. (2021, February 13). Retrieved June 23, 2022, from https://www.jigsawacademy.com/blogs/cyber-security/history-of-cybercrime/.

Hopkins, V. (2022, February 15). *A hack of the Defense Ministry, Army and State Banks was the largest of its kind in Ukraine's history.* The New York Times. Retrieved June 29, 2022, from https://www.nytimes.com/2022/02/15/world/europe/ukraine-cyberattack.html.

How bad are cyberattacks for the economy? This professor helped the White House assess the damage. How bad are cyberattacks for the economy? This professor helped the White House assess the damage. (n.d.). Retrieved June 24, 2022, from https://www.brandeis.edu/global/news/2020/scherbina-q-a.html.

How can countries respond to and deter cyber attacks? - AEI. (n.d.). Retrieved June 26, 2022, from https://www.aei.org/foreign-and-defense-policy/how-can-countries-respond-to-and-deter-cyber-attacks/.

How cyber attacks affect individuals and how you can help keep them safe. ECPI University. (n.d.). Retrieved June 24, 2022, from https://www.ecpi.edu/blog/how-cyber-attacks-affect-individuals-and-how-you-can-help-keep-them-safe.

Howell, C., & West, D. M. (2022, March 9). *The internet as a human right*. Brookings. Retrieved June 27, 2022, from https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/.

Hurst, D. (2019, April 26). *Japan, US beef up their cyber alliance*. – The Diplomat. Retrieved July 10, 2022, from https://thediplomat.com/2019/04/japan-us-beef-up-their-cyber-alliance/.

Innovation and economic growth: Lessons from the story of Eniac. Foreign Policy Research Institute. (2016, August 11). Retrieved June 23, 2022, from https://www.fpri.org/article/2009/04/innovation-and-economic-growth-lessons-from-the-story-of-eniac/.

ITU-D Cybersecurity. ITU Development Cybersecurity. (n.d.). Retrieved July 19, 2022, from https://www.itu.int/itu-d/sites/cybersecurity/.

Johnny 5 on January 5, (2021, October 4). *ExpressVPN: Online privacy is why Sweden wins the internet*. Home of internet privacy. Retrieved July 18, 2022, from https://www.expressvpn.com/blog/online-privacy-is-why-sweden-wins-the-internet/#:~:text=The%20Swedish%20government%20places%20no,monitored%20without%20proper%20judicial%20authorization.

Kaspersky. (2021, May 26). *Kaspersky Lab identifies Operation "Red October," an advanced cyber-espionage campaign targeting diplomatic and government institutions worldwide*. www.kaspersky.com. Retrieved July 1, 2022, from https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide.

Katsh, M. E. (n.d.). *DISPUTE RESOLUTION IN CYBERSPACE*. Dispute resolution in Cyberspace. Retrieved June 26, 2022, from https://www.umass.edu/legal/articles/uconn.html.

Kehoe, B. P. (n.d.). *The Robert Morris Internet Worm*. Research. Retrieved June 29, 2022, from https://groups.csail.mit.edu/mac/classes/6.805/articles/morris-worm.html.

Khalil, A. (2012, December 14). *89 nations sign the controversial UN Telecom Treaty*. Phys.org. Retrieved June 27, 2022, from https://phys.org/news/2012-12-nations-controversial-telecom-treaty.html.

Kramer, A. E. (2017, June 28). *Ukraine cyberattack was meant to paralyze, not profit, evidence shows*. The New York Times. Retrieved July 2, 2022, from https://www.nytimes.com/2017/06/28/world/europe/ukraine-ransomware-cyberbomb-accountants-russia.html.

Lewis, L. (2021, September 11). *Japan is belatedly recognising the risks of Cyber War* . Subscribe to read | Financial Times. Retrieved July 10, 2022, from https://www.ft.com/content/43f7cc53-3ed5-4df9-92fd-3823e36a8f05.

Lovet, G. (2012, September 2). *FIGHTING CYBERCRIME: TECHNICAL, JURIDICAL AND ETHICAL CHALLENGES*. HHS.gov. Retrieved July 19, 2022, from https://web.archive.org/web/20110902091006/http://whitepapers.hackerjournals.com/wp-content/uploads/2009/12/FIGHTING-CYBERCRIME.pdf.

Marks, J., & Schaffer, A. (2022, January 20). *Analysis | Is Russia or China the biggest cyber threat? experts are split*. The Washington Post. Retrieved June 24, 2022, from https://www.washingtonpost.com/politics/2022/01/20/is-russia-or-china-biggest-cyber-threat-experts-are-split/.

Matthews, T. (2022, February 16). *Creeper: The World's first computer virus*. Exabeam. Retrieved June 28, 2022, from https://www.exabeam.com/information-security/creeper-computer-virus/.

National strategies. ITU. (n.d.). Retrieved July 19, 2022, from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

O'Driscoll, A. (2022, May 18). *UK cyber security and Cyber Crime Statistics in 2022*. Comparitech. Retrieved July 18, 2022, from https://www.comparitech.com/blog/information-security/uk-cyber-security-statistics/#:~:text=There%20were%20over%20400%2C000%20reports,individuals%20and%2060%2C111%20from%20businesses.

O'Sullivan, D. (2021, March 26). *Chinese hackers targeted Uyghurs living in us, Facebook Security Team finds*. CNN. Retrieved July 18, 2022, from https://edition.cnn.com/2021/03/24/tech/uyghurs-hacking/index.html.

Page, C. (2021, September 2). *FBI says Chinese authorities are hacking US-based Uyghurs*. TechCrunch. Retrieved July 18, 2022, from https://techcrunch.com/2021/09/02/fbi-china-hacking-uyghurs/.

Page, M. (2022, March 7). *The hypocrisy of Russia's push for a new global cybercrime treaty*. The Interpreter. Retrieved June 30, 2022, from https://www.lowyinstitute.org/the-interpreter/hypocrisy-russia-s-push-new-global-cybercrime-treaty.

Price, G. (2022, June 6). *New Data, statistics: ITU releases 2022 Global Connectivity Report, global potential of internet remains largely untapped*. Library Journal infoDOCKET. Retrieved June 27, 2022, from https://www.infodocket.com/2022/06/06/itu-releases-2022-global-connectivity-report-global-potential-of-internet-remains-largely-untapped/.

Published. (2016, June 10). *The role of Technology*. Knight Foundation. Retrieved June 23, 2022, from https://knightfoundation.org/digitalcitizenship/technology/.

S;, H. (n.d.). *Deindividuation and internet software piracy*. Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society. Retrieved June 27, 2022, from https://pubmed.ncbi.nlm.nih.gov/18721086/.

Saha, B. S. (2022, July 14). *OTP, KYC, pin theft biggest reasons for phishing and cybercrime in India*. MediaNama. Retrieved July 18, 2022, from https://www.medianama.com/2022/07/223-dialogue-report-phishing-cybercrime-fraud-india/.

Saha, B. S. (2022, July 14). *OTP, KYC, pin theft biggest reasons for phishing and cybercrime in India*. MediaNama. Retrieved July 18, 2022, from https://www.medianama.com/2022/07/223-dialogue-report-phishing-cybercrime-fraud-india/.

Sarah Hospelhorn Based in Brooklyn, Hospelhorn, S., Brooklyn, B. in, Sobers, R., & By. (n.d.). *8 events that changed cybersecurity forever*. Varonis. Retrieved June 28, 2022, from https://www.varonis.com/blog/events-that-changed-cybersecurity.

Satter, R. (2020, September 2). *U.S. court: Mass surveillance program exposed by Snowden was illegal*. U.S. Retrieved July 2, 2022, from https://web.archive.org/web/20201101085850/https://www.reuters.com/article/us-usa-nsa-spying/us-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK.

Schwartz, M. J., & Ross, R. (n.d.). *Why Russian cybercrime markets are thriving*. Bank Information Security. Retrieved July 7, 2022, from https://www.bankinfosecurity.com/russian-cybercrime-markets-are-thriving-a-8439.

Security Magazine. (2020, October 23). *UK sees a 31% increase in cyber crime amid the pandemic*. Security Magazine RSS. Retrieved July 18, 2022, from https://www.securitymagazine.com/articles/93722-uk-sees-a-31-increase-in-cyber-crime-amid-the-pandemic.

Sinha, J. (2022, July 18). *New Challenge for Delhi Cyber Unit: Crypto*. The Indian Express. Retrieved July 18, 2022, from https://indianexpress.com/article/cities/delhi/new-challenge-for-delhi-cyber-unit-crypto-8035547/.

Stupples, D. (2015, November 27). *The next big war will be digital-and we're not ready for it*. Gizmodo. Retrieved June 24, 2022, from https://gizmodo.com/the-next-big-war-will-be-digital-and-we-re-not-ready-fo-1744865435.

Sweden's digital technologies ecosystem. Sweden's Digital Technologies Ecosystem - Business Sweden. (n.d.). Retrieved July 18, 2022, from https://www.business-sweden.com/markets/sweden/swedens-digital-technologies-ecosystem/.

Techopedia. (2011, August 18). *What is a creeper virus? - definition from Techopedia*. Techopedia.com. Retrieved June 28, 2022, from https://www.techopedia.com/definition/creeper-virus.

Teti, A. (n.d.). *Operation 'red october': And it is Cyber Espionage*. GNOSIS. Retrieved July 2, 2022, from https://gnosis.aisi.gov.it/gnosis/Rivista34.nsf/ServNavigE/34-09.pdf/$File/34-09.pdf?OpenElement.

Tidy, J. (2022, February 14). *74% of ransomware revenue goes to Russia-linked hackers*. BBC News. Retrieved July 7, 2022, from https://www.bbc.com/news/technology-60378009.

Tripwire Guest AuthorsAug 17, 2016F. A. (2016, August 17). *The evolution of hacking*. The State of Security. Retrieved June 23, 2022, from https://www.tripwire.com/stateofsecurity/securitydataprotection/cyber-security/the-evolution-of-hacking/.

UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed Outcomes for Human Rights Online. UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online | Association for Progressive Communications. (n.d.). Retrieved June 24, 2022, from https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed.

United Nations. (n.d.). *About the International Telecommunication Union (ITU)*. ITU. Retrieved June 27, 2022, from https://www.itu.int/en/about/Pages/default.aspx.

United Nations. (n.d.). *Developments in the field of information and telecommunications in the context of international security :* United Nations. Retrieved June 24, 2022, from https://digitallibrary.un.org/record/265311?ln=en.

United Nations. (n.d.). *Global cybersecurity agenda (GCA) - united nations office on drugs and ...* International Telecommunications Union. Retrieved June 27, 2022, from https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/Presentations/ITU_Cybercrime_EGMJan2011.pdf.

United Nations. (n.d.). *International human rights law*. OHCHR. Retrieved June 27, 2022, from https://www.ohchr.org/en/instruments-and-mechanisms/international-human-rights-law.

United Nations. (n.d.). *Unidir: The humanitarian impact of cyber attacks against Critical Infrastructure (4 July 2022)*. United Nations. Retrieved June 26, 2022, from https://indico.un.org/event/38035/.

The United States Government. (2022, March 21). *Statement by president Biden on our nation's cybersecurity*. The White House. Retrieved June 23, 2022, from https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.

UNODC. (n.d.). *Comments on China*. UNODC. Retrieved July 10, 2022, from https://www.unodc.org/documents/Cybercrime/English.pdf.

Use of the internet. United Nations : Office on Drugs and Crime. (n.d.). Retrieved June 26, 2022, from https://www.unodc.org/unodc/en/terrorism/news-and-events/use-of-the-internet.html.

Wakefield, J. (2017, June 28). *Tax software blamed for cyber-attack spread*. BBC News. Retrieved July 2, 2022, from https://www.bbc.com/news/technology-40428967.

Watering, J. van de. (2020, March 5). *The origin of cybercrime - goose VPN*. GOOSE VPN service. Retrieved June 23, 2022, from https://goosevpn.com/blog/origin-cybercrime.

What is a VPN? virtual private network meaning. NordVPN. (2022, June 23). Retrieved June 26, 2022, from https://nordvpn.com/what-is-a-vpn/.

What is Cyberspace. IGI Global. (n.d.). Retrieved June 22, 2022, from https://www.igi-global.com/dictionary/cybersecurity-new-challenge-information-society/6619.

What is stuxnet? Trellix. (n.d.). Retrieved June 24, 2022, from https://www.trellix.com/en-us/security-awareness/ransomware/what-is-stuxnet.html.

What is the Morris Worm? history and modern impact. Okta. (n.d.). Retrieved June 29, 2022, from https://www.okta.com/identity-101/morris-worm/#:~:text=TheMorriswormwascreatedbyaprankster.

Why do we fall for scams? - JSTOR DAILY. (n.d.). Retrieved June 23, 2022, from https://daily.jstor.org/why-do-we-fall-for-scams/.

Wigan Council. (n.d.). Cyber terrorism. Retrieved June 26, 2022, from https://www.wigan.gov.uk/Resident/Crime-Emergencies/Counter-terrorism/Cyber-terrorism.aspx.

秦琪. (n.d.). *China handles 62,000 cybercrime cases in 2021*. The State Council Information Office of the People's Republic of China. Retrieved July 10, 2022, from http://english.scio.gov.cn/pressroom/2022-01/06/content_77972842.htm.