Data Privacy Summit Background Guide

Written by: *Tharun Viswanathan, Case Western Reserve University*

Written December 2023

The Data Privacy Summit is a group of nations convened through the International Association of Privacy Professionals (IAPP) designed to tackle the complexities of data privacy. It acts as a consultant to the United Nations in this matter and functions as a sub-body of the General Assembly. In this digital age, the protection of personal information is a pertinent matter for both the individual and the state, prompting the necessity for global collaboration. This summit provides a platform for delegates to engage in meaningful discussions, share diverse perspectives, and address the challenges posed by the interconnected world. As we navigate the expanding digital landscape, the need for a robust data protection framework has become evident. Throughout this conference, delegates are expected to work together to formulate resolutions that respect national sovereignty while upholding the fundamental right to privacy in a globally integrated society.

I. Regulating Transnational Data Flow

Statement of the Issue:

Digital transformation is one of the key trends of the 21st century and has been further catalyzed through the COVID-19 pandemic, which encouraged internet-dependent actions such as remote working and advancement of social media urging all governments to respond to the surge in internet traffic. The 2021 Digital Report cites that the global traffic in 2022 has exceeded previously recorded amounts until 2016, and is continually increasing especially with the introduction of Artificial Intelligence and Machine Learning.[1] Furthermore, the significant traffic growth has yielded technological discrepancies among nations of the world, with Least Developed Countries (LDC) having minimal broadband access, limiting their access to the global digital network This has further contributed to the socio-economic challenges present in the world, as an unequal access to the data flow largely prevents a developing country's commercial success. Only 20 percent of people in LDCs have access to the internet, and that too is also limited, characterized by low download speeds and high cost. The countries that have the greatest data flow also house major companies that specialize in data collection and digital technology. Two notable nations are the United States and China, which account for half the world's data centers, the fastest adoption and subsidization of 5G, 94% of global Artificial Intelligence startups, and 70% of AI researchers. Such statistics have further contributed to the global wealth gap, hindering a more collective global recovery

[1] ("Digital Economy Report 2021 | UNCTAD")

from the COVID-19 pandemic. As the digital economy has evolved, a new system has risen with LDCs providing raw data to corporations.

The 2030 Agenda for Sustainable Development aims to mitigate the inequalities that are present in the world, including internet access for every person.[2] It has become increasingly significant to focus on data governance, as the current fragmented netscape hinders a more comprehensive and collaborative usage of existing public data, and also provides a greater risk in terms of privacy breaches and cybercrimes. United Nations Conference on Trade and Development (UNCTAD) Secretary-General Rebeca Gryspan states that the issue of digital governance can no longer be postponed, with potential applications including the health sector where a more organized data flow is needed for a better-coordinated counter to epidemics as well as much more rapid vaccine development.[3] With the rise of Artificial Intelligence and its ability to freely access data, it is important to democratize its usage. This has yielded concerns regarding privacy and security as many countries are still skeptical about reducing the barriers to enable data flow. This hesitation has decelerated the global deployment of AI, forcing organizations to duplicate it instead, costing extra time and money. Hence, to fully reap the benefits of AI and the international flow of data, the United Nations has called upon several international organizations to create a more interoperable framework that enables cross-border data flow, such as the Data Privacy Summit.[4]

History:

Between 1970 and the 1980s, a variety of European countries adopted data protection laws with clauses addressing transborder data flow. The primary concern at the time was the circumvention of data laws by transferring valuable data to another country without stringent data protection laws. Clauses ranged from a permit from authorities to transfer data outside the country, as documented in early Swedish and Austrian law, to consent from the subject whose data was being transferred.[5]

The Organization for Economic Cooperation and Development's Data Privacy Guidelines represented the first regulation of transborder data flow from a global perspective. Adopted in 1980, the guidelines were a set of non-binding principles that countries chose to enact to create a respectable standard for data protection while still allowing the potential of cross-border data flow. The guidelines contained the following provisions regarding transnational data flow:

- Member countries are expected to consider in their legislation the implications for other member countries of domestic regulation and the re-export of personal data.

[2] ("Digital Economy Report 2021 | UNCTAD")
[3] ("New approach needed to make digital data flow beneficial for all")
[4] (Marwala et al.)
[5] (Kuner)

- Member countries should take reasonable and appropriate measures to ensure that transnational data flows are uninterrupted and secure.
- Member countries should restrict cross-border data flow only when the recipient country does not obey the guidelines or when the re-export of data disobeys the sender country's domestic guidelines.
- Member countries should refrain from developing laws which act as an obstacle to transborder flow.[6]

In 1990, the United Nations drafted its Guidelines on Computerized Personal Files, which is a non-binding guidance document regarding digital privacy. It contains two clauses which address transborder data flow:

- Article 28 of the Introduction: The national rules relating to the protection of personal data should not unduly restrict the freedom to seek, receive, and impart information regardless of frontiers, as provided in Article 19 of the International Covenant on Civil and Political Rights. This is especially true when the legislation of the countries concerned by the flow offers equivalent safeguards in respect of the protection of privacy.
- Annex I Article 9: When the legislation of two or more countries concerned by a transborder data flow offers more or less equivalent safeguards for the protection of privacy, information should be able to circulate as freely as inside one of the territories. If there are no reciprocal safeguards, limitations can only be provided when there is a clear violation of privacy.[7]

In 2018, the United Nations adopted the Principles on Personal Data Protection and Privacy, which focused on the protection of human rights concerning privacy when it came to the transfer of information across United Nations System Organizations. The document calls for the fair and legitimate processing of personal data on the following legal bases:

- Consent from the data subject: the most common legal basis for data processing.
- The best interest of the System Organizations: in some cases, UN organizations are allowed to process data without consent if it is determined to be in their best interest. Such situations include the protection of an individual.
- Mandates and governing instruments of the System Organizations: similar to the previous point, data collection may be an integral aspect of an organization's proper functioning.

[6] (Kuner)
[7] (Joinet)

- Any other legal basis: The organizations can identify other specific legal grounds for the collection of personal data which could entail national laws, agreements, or specific legal provisions.[8]

In the same year, the UN Secretary-General assembled a panel focused on the advancement of cooperation among entities in the digital space. The panel was chaired by Melinda Gates and Jack Ma, and while focusing on a variety of digital issues, they focused on providing suggestions on the topic of transnational data flow through the creation of a platform for the sharing of public goods, engaging talent, and pooling data sets through a broad multidisciplinary alliance involving the United Nations and an expedited consultation process. These ideas were intended to develop updated mechanisms for global digital cooperation. The panel suggested three potential solutions: the first being an enhanced internet governance forum (IGF). enhanced through the IGF+ model. The second, a co-governance (COGOV) model which would link existing institutions and assign roles for each with regards to digital governance. This model would be built on existing mechanisms stated earlier with an expectation to create new solutions to address existing gaps in transnational data flow. The third would be a Digital Architecture model which would be a set of shared principles and norms for the management of digital resources. After the panel discussion, 8 more conferences occurred between various stakeholders discussing the issues put forth by the panel. This resulted in the creation of the Roadmap for Digital Cooperation.[9]

Analysis:

One of the biggest challenges that the Data Privacy Summit faces is the balance between Data Sharing and Data Privacy. Data protection laws are tasked with safeguarding individual sovereignty, yet may be excessive in many cases, which restricts the flow of information hindering data sharing and subsequent innovation on a global scale. Conversely, inadequate identity protection may cause the personal information of individuals to be unauthorized or misused. This struggle for balance is worsened by the lack of transparency and accountability of nations surrounding cross-country data flow. The Summit is thus tasked to consider and develop practices that are properly justified, as individuals may not understand the reasoning behind such practices. Such practices may go so far as to hold international entities accountable for data privacy violations. Another problem the Summit faces is ensuring the harmony between current regulations and the ones that are to be drafted. Ensuring that organizations comply with laws across different jurisdictions is challenging, especially in a globalized digital landscape. Differences in data protection laws, legal systems, and the decentralized nature of the internet make it difficult to enforce compliance consistently. Moreover, limited enforcement capabilities and cooperation amongst countries provide greater obstacles in enforcing regulation.

[8] ("Principles on Personal Data Protection and Privacy")

[9] ("Roadmap for digital cooperation")

The Data Privacy Summit is delegated with the aforementioned responsibilities alongside a minimally unified global framework, aggravated by the fragmented regulations across countries. Unfortunately, organizations have taken advantage of the lack of cooperation to operate across borders. The Summit must also recognize existing data localization requirements calling for certain data to remain and classified within certain borders. For a global framework to be successful, it must satisfy the localization requirements.

Finally, the Summit must consider the development of new technology. The emergence of sophisticated data processing techniques alongside the increasing volume and complexity of data has made it difficult to keep data protection laws up to date. Resolutions drafted by the Summit should adapt to these changes to ensure effective protection of data privacy and security.

Conclusion:

Regulating transnational data flow is a complex issue that must be addressed on multiple levels and consider the various complexities. The purpose of the Data Privacy Summit is to draft an internationalnframework, recognized by as many countries as possible, which means comprehensively adhering to their data localization requirements. At the same time, the Summit should recognize that new methods of data flow are currently being developed and must ensure that their resolution has postulates to combat this very issue. Finally, the Summit must address the gap in data transfers across the world, focusing on enabling LDCs to gain greater access to global data transfer.

References:

"Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow | General Assembly of the United Nations." *the United Nations*, 14 December 2021, https://www.un.org/pga/76/2021/12/14/unctad-digital-economy-report /.

Joinet, Louis. "Guidelines for the Regulation of Computerized Personal Data Files:" *United Nations Digital Library System*, 1988, https://digitallibrary.un.org/record/43365?ln=en .

Kuner, C. (2011), "Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future", OECD Digital Economy Papers, No. 187, OECD Publishing, Paris, https://doi.org/10.1787/5kg0s2fk315f-en .

Marwala, Tshilidzi, et al. "Regulating Cross-Border Data Flows: Harnessing Safe Data Sharing for Global and Inclusive Artificial Intelligence." *United Nations University*, 26 October 2023, https://unu.edu/publication/regulating-cross-border-data-flows-harnessing-safe-data-sharing-global-and-inclusive .

"New approach needed to make digital data flow beneficial for all." *UN News*, 29 September 2021, https://news.un.org/en/story/2021/09/1101542.

"Roadmap for digital cooperation." *Digital Watch Observatory*, 11 June 2020, https://dig.watch/processes/roadmap .

"Principles on Personal Data Protection and Privacy." *United Nations* - *CEB*, https://unsceb.org/principles-personal-data-protection-and-privacy-listing.

II. Countering Cyber Espionage by Non-State Actors

Statement of the Issue:

The United Nations Office on Drugs and Crime (UNODC) defines cyber espionage as the use of information and communication technology (ICT) by individuals, groups, or businesses for some economic or personal gain. They also state that it can be carried out by government actors, defined as a state-sponsored or directed group seeking to gain unauthorized access to systems and data in a bid to collect intelligence on a target country to boost their own national security, economy, or military strength.[10] While espionage has existed for a long time, technology is now being used to establish a tactical advantage, enabling illicit intelligence connections at an unprecedented rate while mitigating the chances of being associated with a particular source. The UN has associated multiple cyber espionage campaigns with Advanced Persistent Threats (APTs), groups with the capability and intent to target a national entity. These groups use a plethora of methods to engage in cybercrime which include, but are not limited to:

- Malware: Software that is specifically designed to damage a particular system. For example, a piece of software known as Flame was known to obtain data from a victim system by remotely controlling the webcam and microphone. The software was also able to take screenshots of the computer.
- Social Engineering: The attacker gains access to information by convincing the victim to give the information directly or by other methods. A common technique involved in social engineering is spear phishing, where emails with a fake link designed to appear real are sent to the target, in the hopes that the target clicks on the link granting the perpetrator access to the victim's computer.
- Watering Hole Attack: Perpetrators monitor websites commonly used by many people and then infect them with spyware to gain access to their network. One way this attack can be done is by recreating a website and routing target users to it.
- Sometimes people who already exist within the organization serve as a method, by intentionally or unintentionally disclosing information to the actor.

With how nuanced the internet has become, cyber espionage has been made easier through the variety of tools available online. These tools include zero-day hacks, formerly unknown vulnerabilities that are either exploited to bypass firewalls, allowing access to confidential information, or implants, essentially serve as secret portals that may be strategically placed to gain unauthorized access.[11]

Cyber espionage is mainly targeted at large corporations, government agencies, academic institutions, or other organizations that possess valuable data, such as research material, intellectual property, political strategies, and military information. Sometimes cyber espionage is also conducted

[10] ("Cybercrime Module 14 Key Issues: Cyberespionage")
[11] ("Cybercrime Module 14 Key Issues: Cyberespionage")

against specific individuals such as government officials or celebrities. Cyber espionage is also conducted sometimes to tarnish the reputation of certain individuals or nations. It can be developed in conjunction with the military as a method of cyber terrorism or warfare. Its effects can range from the destruction of public services to the loss of life.[12]

Due to how covert cyber espionage is, it is difficult for daily users to understand its impacts. However, when conducted on a greater scale, the effects of cyber espionage can severely and directly affect many lives across the world. The values of assets listed above usually range in the millions of dollars, therefore strongly suggesting a steep economic consequence on the victim nation. Washington University in St. Louis theorizes losses from cyber espionage to be in the tens of millions of dollars in the US alone, while the Center for Strategic and International Studies reports global losses to be at least $600 billion.[13]

However, there may be justification behind the lack of regulations regarding cyber espionage affecting daily life. Some analysts argue that cyber espionage is too disjointed and disorganized to be considered a real war, which can comparatively yield much higher collateral damage. Often cyber espionage is stopped before a great amount of damage is done. Regardless, the media tends to sensationalize incidents, causing a rise in paranoia regarding the destruction that may be brought forth by cyber-attacks. Early data shows that a mere 3% of all cyber-attacks could not be stopped, with smaller data companies being targeted. However, in the modern era, actors can equip themselves with advanced technology to the point that they can be considered security threats[14]. Hence, the Data Privacy Summit is responsible for creating a resolution that can counter cyber espionage with the capability of resulting in tangible damage worldwide.

History:

Due to how concealed many of the operations are, it is difficult to trace when the first act of cyber espionage was conducted. The first documented and widespread cybersecurity attack was Moonlight Maze in 1999, a Russian government-sponsored assault on the US. Moonlight Maze targeted NASA, the Pentagon, military contractors, civilian academies, and many more American departments. The threat actors routed communications through a third-party server to avoid detection and built back doors into systems so they could go back in later to obtain data. The attack was carried out over two years and was categorized as an advanced persistent threat (APT) because it was so difficult to detect. Its damage, in contrast, was in the millions according to James Adams, CEO of Infrastructure Defense Inc. Information recovered in the hack included classified naval codes, data on missile-guidance systems, and other highly valued military

[12] (Baker)
[13] (Rubenstein)
[14] (Rubenstein)

information. The attackers also stole tens of thousands of files that included technical research, military maps, U.S. troop configurations, military hardware designs, encryption techniques, and data relating to the Pentagon's war planning, all of which could be sold in illegal underground markets.[15]

Some more recent examples of Cyber espionage include:

- **Stuxnet attack on Iran's nuclear program**: Believed to be a joint effort by the United States and Israel agencies in 2010, Stuxnet was a worm that attacked the centrifuges that were used to enrich the Uranium for the development of Iranian nuclear weapons. It exploited multiple zero-day bugs in the Windows operating software that was used in the Siemens programmable logic controller utilized in the centrifuge. The attack was successful, allowing the United States to retain its advantage in the development and retention of nuclear weapons as opposed to Iran, which was attempting to build its nuclear arsenal.[16]
- **Cozy Bear**: Categorized as APT29, Cozy Bear is an organization that is affiliated with Russia's Foreign Intelligence Service. They have been active since 2008, mainly targeting European government networks. Cozy Bear infiltrated the SolarWinds supply chain in 2020, compromising the software used by thousands of organizations, including government agencies and Fortune 500 companies in the United States. The attack allowed the group to gain access to sensitive data and potentially monitor the communications of government officials. In 2016, Cozy Bear also launched the VPNFilter attack, which targeted government and military networks worldwide. The attack used malware to infiltrate network routers and potentially steal data or disrupt operations.[17]
- **DarkTequila**: DarkTequila is a cyber espionage campaign conducted by unknown actors that mainly targeted the financial sector of Mexico. Attacking 30,000 users in 2018, the actors used spear phishing to steal a great amount of data before using a USB infector to spread across offline channels.[18]

The United Nations Office on Counter-Terrorism (OCT) has launched several initiatives in the field of cybersecurity and is working toward developing new technology to counter cyber espionage. The Global Counter-Terrorism Programme on Cybersecurity and New Technologies was adopted in April 2020, providing member states with the means to develop and implement effective measures to protect themselves from cyber-attacks. This program is based on Pillar 2 of the Global Counter-Terrorism Strategy and implements its aims by:

[15] (Miller)

[16] (Fruhlinger)

[17] (Temple-Raston)

[18] (Madsen)

- Developing knowledge and raising awareness of the challenges and opportunities related to new technologies for countering terrorism;
- Enhancing skills required to develop and implement effective national counter-terrorism policy responses to the challenges and opportunities brought forth by new technologies;
- Enlarging capacities required to protect critical infrastructures against terrorist cyber-attacks;
- Improving criminal justice enforcement to counter and investigate terrorist use of new technologies.

The program was able to train over 3300 officials from a variety of member states.[19]

The OCT, alongside the International Criminal Police Organization (INTERPOL), released the Counter Terrorism Tech Initiative, focusing on the strengthening of law enforcement and justice systems in certain countries to counter the exploitation of new technologies that can be used as vectors of cyber espionage. The program also focused on mitigating damage and redevelopment of infrastructure in the event a system was attacked by a hostile actor. The initiative contained 5 phases:

- **Inception**: OCT and INTERPOL convened with partner states to better understand the necessity for building counterterrorism measures.
- **Knowledge Development**: The initiative focused on distributing knowledge on cybersecurity protection among the tested member states.
- **Awareness Building**: States expanded their knowledge and strengthened preparations for countering cyber espionage, by conducting a thorough national threat assessment, developing countermeasures, and assessing law enforcement capabilities.
- **Training and Closing:** Each member state was trained based on the knowledge development and awareness-building aspects. Furthermore, the results from the training were assessed by the UNOCT and Interpol .[20]

The UNOCT also provides expertise in international fora on the use of unmanned aerial systems (UAS) and delivers capacity-building assistance in Open-Source Intelligence (OSINT), the dark web, cryptocurrencies, and digital forensic investigations with past UNOCT projects. Such projects include focusing on the use of social media to gather open-source information and digital evidence to counter terrorism and violent extremism while respecting human rights. The United Nations is currently still negotiating a formally recognized international treaty countering cybercrime. If it passes, it would be regarded as the first internationally binding treaty on the topic of cybercrime.

At the moment, regulation of information privacy and solutions to counter cyber espionage remain limited to regional documentation. One example is the General Data Protection Regulation (GDPR), drafted by the European Union. It is a set of laws that can be imposed on global organizations that are focused on

[19] ("Cybersecurity and New Technologies | Office of Counter-Terrorism")
[20] ("CT TECH Initiative | Office of Counter-Terrorism")

the protection of data, as well as the punishment that perpetrators should get if they break any of the laws dictated in the document. While not directly referencing it, the GDPR also addresses parts of cyber espionage through articles such as:

- Article 5: deems that personal data shall be collected for specific, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes. Subclause f also calls for personal data to be processed in a manner that guarantees security from unlawful processing, which includes cyber espionage.
- Article 32: calls for the measures required to protect personal data in conjunction with Article 5. Some examples listed include the encryption of data, ensuring ongoing confidentiality, the ability to restore data in case of an incident, and regularly testing the proper functioning of the implementations. The GDPR also gives guidelines dictating the level of protection required based on a risk assessment of how much of the data can be lost.
- Article 33: necessitates that any incidents of data breaches (which may include cyber espionage) must be reported within 72 hours. The report should include the nature of the breach that occurred, the likely consequences of the breach and the measures to be taken to address the breach, including methods to mitigate its effects.
- Article 34: calls to report data breaches to subjects whose data might be compromised. Similar to Article 33, the report should contain a description of the nature of the attack, direct consequences, and means to handle the breach.
- Article 35: requires that organizations conduct a Data Protection Impact Assessment when certain methods of data processing might involve new technology, which could result in the compromise of data.[21]

Outside of the European Union, some examples of regional directives tasked with combating cyber espionage include:

- Organization of American States (OAS) - Inter-American Committee against Terrorism (CICTE) - coordinates efforts amongst the OAS to develop measures against terrorism, the broad spectrum under which cyberterrorism and cyberespionage fall. Specifically, the cybersecurity program focuses on policy development, capacity building, and research awareness raising.[22]
- African Union Convention on Cyber Security and Personal Data Protection - aims to address regulatory issues in the African subcontinent as a result of increased cybercrime.[23]

[21] General Data Protection Regulation (GDPR)
[22] ("OAS :: CICTE: Cybersecurity")
[23] (Kaaniru)

- ASEAN Regional Forum Work Plan on Practical Measures to Enhance Confidence and Prevent Incidents in Cyberspace. - It aims to promote transparency and develop confidence-building measures to increase understanding among countries of the technological environment to mitigate misperception. It also aims to raise awareness of threats related to technology and strengthen cooperation between the countries in the forum to better counter cyber threats.[24]

Analysis:

The United Nations has deemed countering cyber threats to be the top priority for safe and positive technological development around the world. For an effective countermeasure, member states need to first identify non-state actors that have and could act as threats in the future. This action also calls for global cooperation to provide targeted countries with the resources they need not only to investigate for threats but also to arm themselves in the event of a future breach. It is difficult, however, for the proper development of a defensive system as the recent development of the internet and its technological tools have made it much easier to attack individuals and states than to defend. Anonymity enables not only organizations but also individuals to engage in espionage without having to reveal themselves. The attacking body uses a variety of anonymization techniques to cover their identity and actions. The pursuit and success of maintaining anonymity is unfortunately further enhanced through the usage of zombie computers, which are digital devices controlled by a third party and are typically used as a method to access sensitive information from another device that has been infected with malware[25]. However, states should consider that anonymity also protects individuals and privacy. The Data Privacy Summit is expected to take account of existing technology enabling non-state actors to successfully commit cyber espionage and should aim to create regulations to mitigate the harmful potential the actors hold.

The Summit will also have to work on balancing cyber security with privacy. Outside of personal privacy, state sovereignty also plays a big part. As a result, defining what constitutes a violation of sovereignty in cyberspace can be contentious, which has previously led to roadblocks in the development of international protocol concerning cybercrime. Achieving consensus on norms and rules for countering cyber espionage can be challenging, particularly if there are geopolitical tensions among member states. As a result, states may have divergent views on what actions are acceptable in cyberspace. Thus, the Summit is expected to create a document that remains relevant throughout the course of time and considerate of the diverse viewpoints across nations. This means creating a document that handles the technicalities of cyberspace, while being viable to policymakers at the same time, which means succinctly enforcing any laws that may be created without immediately resorting to harsh disciplinary action.

[24] ("13-1 ARF ICT work plan 7 May 2015 FINAL")

[25] ("Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations")

Conclusion:

Cyber espionage is a growing threat affecting all nations, with many non-state actors attempting to gain leverage by compromising target countries. The Data Privacy Summit is expected to address the methods that actors use to steal information through the creation of a detailed guide that equips countries with the means to protect themselves from attacks, identify sources of threats, and rebuild technological infrastructure if an attack is conducted. The Summit must further harmonize existing regional laws to form an international agreement that enables the United Nations to govern, identify, and properly handle cyber threats.

References:

Baker, Kurt. "What is Cyber Espionage? – CrowdStrike." *CrowdStrike*, 28 February 2023, https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

"CT TECH Initiative | Office of Counter-Terrorism." *the United Nations*, https://www.un.org/counterterrorism/ct-tech-initiative.

"Cybercrime Module 14 Key Issues: Cyberespionage." *UNODC*, https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberespionage.html.

"Cybercrime Module 5 Key Issues: Obstacles to Cybercrime Investigations." *UNODC*, https://www.unodc.org/e4j/zh/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.

"Cybersecurity and New Technologies | Office of Counter-Terrorism." *the United Nations*, https://www.un.org/counterterrorism/cct/programme-projects/cybersecurity .

Fruhlinger, Josh. "Stuxnet explained: The first known cyberweapon." *CSO Online*, 31 August 2022, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html .

Madsen, Connor. "Cyber News Rundown: Dark Tequila Malware." *Webroot*, 24 August 2018, https://www.webroot.com/blog/2018/08/24/cyber-news-rundown-dark-tequila-malware/.

Miller, Christina. "Throwback attack: Russia launches its first cyberattack on the U.S. with Moonlight Maze | Industrial Cybersecurity Pulse." *Industrial Cybersecurity Pulse*, 10 March 2022, https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-russia-launches-its-first-cyberattack-on-the-u-s-with-moonlight-maze/.

Rubenstein, Dana. "Nation-State Cyber Espionage and its Impacts." *Computer Science & Engineering*, 1 December 2014, https://www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/.

Temple-Raston, Dina. “How Russia Used SolarWinds To Hack Microsoft, Intel, Pentagon, Other Networks.” *NPR*, 16 April 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

General Data Protection Regulation (GDPR) – Official Legal Text, https://gdpr-info.eu/ .

“OAS :: CICTE: Cybersecurity.” *Organization of American States*, https://www.oas.org/en/sms/cicte/prog-cybersecurity.asp.

Kaaniru, Josephine. “The African Union Convention on Cyber Security and Personal Data Protection: Key Insights - Centre for Intellectual Property and Information Technology Law.” Centre for Intellectual Property and Information Technology law, 24 July 2023, https://cipit.org/the-african-union-convention-on-cyber-security-and-personal-data-protection-key-insights/.

“13-1 ARF ICT work plan 7 May 2015 FINAL.” Asean Regional Forum, https://aseanregionalforum.asean.org/wp-content/uploads/2018/07/ARF-Work-Plan-on-Security-of-and-in-the-Use-of-Information-and-Communications-Technologies.pdf.