QUEEN MARGARET'S SCHOOL

Disarmament and International Security Committee

BACKGROUND GUIDE

QueenMUN 2026

Dear Delegates,

My name is Bronwyn Ellis and I have the honour and privilege to serve as the Director of DISEC for this iteration of QueenMUN. As a Grade 11 at St. Michaels University School in Victoria, this marks my fourth and penultimate year of High School Model United Nations and I hope to bring my love of international relations and debate to all delegates in attendance this year. Myself, your Chair Johan Kim, and Assistant Director Naya Swamy, have been working hard to create an incredible committee for you all this year. Whether you are a seasoned gavel hunter or your first of many conferences to come I hope that you all will enjoy MUN as much as I have over the past four years.

Like many of you, I started Model UN in middle school going to Shawnigan Lake's Global Goals conference. I think I only spoke once with shaky hands and a pile of printed out news articles, but I'd like to say that those days are over as I go into my fourteenth conference. My most treasured memories of MUN come not from moderated caucuses and two hour long committee sessions, but rather the close friends that I've made during breaks and delegate socials. Despite not seeing each other frequently, those friendships are ones that remain close to my heart, and I hope that each and every delegate makes a new friend or two in DISEC this year. When not in western business attire, you can probably find me dressed in black in the wings or tech booth of a theatre, on stage playing violin in orchestra, or reading in bed into the late hours of the night.

This year's topic of Cybersecurity and the Prevention of Cyber Warfare presents a challenge to delegates to find a balance between human and digital rights, and the protection of citizen's data in an ever changing digital world. With the vast majority of the world's population using the internet and/or social media, it is vital that their data is protected and that they feel safe online. At the same time, it is of vital importance to ensure that citizens can voice their opinions and not feel restricted by censorship. It is the duty of delegates in DISEC this year to find a balance and solve this prevalent issue.

I wish all delegates good luck in their research and preparations and I eagerly await a conference full of heated debate. If you have any questions or concerns, please feel free to contact me at bronwyn.ellis@smus.ca. On behalf of myself and fellow dais members, welcome to DISEC.

Sincerely,

Bronwyn Ellis
DISEC Director

Position Paper Policy

What is a Position Paper?

A position paper is a brief overview of a country's stance on the topics being discussed by a particular committee. Though there is no specific format the position paper must follow, it should include your country's background and history on the topic, any political and foreign policy on the topic, any governmental actions related to the topic, and potential solutions your government might suggest. Each position paper should not exceed one page, excluding works cited, and should all be combined into a single document per delegate (for double delegations this means only one delegate needs to submit the paper for both). For DISEC, position papers, although strongly recommended, are not required. However, delegates who wish to be considered for an award must submit position papers. If delegates choose to write their position paper with the help of AI, they will also not be eligible to receive awards.

Formatting

Position papers should:
— Include the name of the delegate, their country, and the committee
— Be in a standard font (e.g. Times New Roman) with a 12-point font size and 1-inch document margins
— Not include illustrations, diagrams, decorations, national symbols, watermarks, or page borders
— Include citations and a bibliography, in any format, giving due credit to the sources used in research (not included in the 1-page limit). Citation style is not standardised
— Not be written by Large Language models (AI)

Due Dates And Submission Procedure

Position papers for this committee must be submitted by **11:59 PM PST on March 5rd, 2026**. Once your position paper is complete, please save the file as your **last name, your first name** (ex. Doe, Jane) and send it as an attachment in an email to your committee's email address, with the subject heading as "**Last Name_First Name_Committee_Position-Position Paper**" ex. Doe_Jane_DISEC_Saudi Arabia-Position Paper. Please do not add any other attachments to the email.
Your position paper should be submitted in **PDF format**; position papers submitted in another format such as a google or Word document will not be accepted. Each position paper will be manually reviewed and considered for the Best Researched award.

Please send all Position Papers to bronwyn.ellis@smus.ca

Overview

The digital world, otherwise known as cyberspace, is a man-made environment that exists beyond the physical borders states have created. Due to the border-less nature of cyberspace, it presents a threat to national sovereignty and a territory where laws vary and do not apply to everything and everyone making regulation very difficult. When an entity attacks cyberspace, it is classified as a cyberattack, however identifying who or what committed the crime is difficult. Virtual Private Networks (VPNs) can mask the location from which an internet user uses and can potentially commit cyberattacks against another user or platform. Attributing cyberattacks to another country is also a major issue as seen by the United States (US) attributing a Sony Pictures hack to North Korea in 2014.[1] While it is widely believed by the international community that North Korea hired a person/people or committed the cyberattack themself, that is not always the case and can result in increased tensions between countries involved.

Cybersecurity is "the practice of protecting computer systems, networks, programs, and data, specifically from digital attacks, unauthorized access, damage, or theft".[2] For many governments, cybersecurity is primarily used to keep classified information, just that, classified. For others, cybersecurity is taken to an extreme, sometimes considered to be taken beyond simple security, by censoring information that is consumed by their citizens. While some argue that this is a measure of protection for the cybersecurity of their citizens, others say that it is a violation of human rights.

Sovereignty is another major concern voiced by the international community in respect to cybersecurity. Cyber sovereignty, defined as "the will of states to exercise and sustain control over the Internet domain within their own borders, including political, economic, cultural and technological activities" is one of the biggest factors in deciding international law on cybersecurity and preventing cyberattacks.[3] United Nations resolutions are not binding to all member countries and only apply to countries that chose to adopt them which means that even if most countries adopt a policy on cybersecurity, once information or data enters the cyberspace of a country that may not have the same policies, data can be used in whatever way by that country.

Above all else, the safety of civilians is of utmost importance, including their personal data. In the past year (2025-2026), 4,100 breaches were reported and on average it took companies nearly 250 days to identify and contain the breach.[4] Around 12 universities experienced data breaches and the United States Congressional Budget Office as well as Union County experienced data breaches, leaking sensitive government data.[5] While it costs corporations several billion dollars

[1] Lee and St. James, "The 2014," Vox
[2] Nason, "A History," Coro
[3] Can, "Grey Zone," abstract
[4] "Recent Breaches," Breachsense
[5] "Data Breaches," *PKWARE* (blog)

to repair leaks, personal information including names, addresses, and government issued identification are shared on the internet, placing millions of people at risk making it imperative that this committee comes to to a resolution

Timeline

Late 1960s - Advanced Research Projects Agency Network (ARPANET) was developed by the United States Department of defense and was essentially the first internet.[6] ARPANET was developed to connect computers at different institutions, however it also included email and file transfer.[7] Considered by many to be the most important technological advancement in computing, ARPANET was the start of cyberspace.

1971 - The first instance of a computer worm was created called Creeper displaying "I am the creeper, catch me if you can". The impact was limited, infecting no more than 28 computers, however it also led to the creation of the first anti-virus called Reaper.[8]

1982 - "Elk Cloner [was] the first personal computer virus or self-replicating program known to have spread in the wild on a large scale".[9] It was created by a 15 year old and spread through floppy disks on Apple II computers, from infected to uninfected.[10] Aside from annoying messages, the virus was relatively harmless.

1986 - "The Computer Fraud and Abuse Act (CFAA) was enacted … as an amendment to the first federal computer fraud law, to address hacking".[11] The CFAA in the United States was one of the first national laws passed by a country to address cyber threats and promote cybersecurity. The CFAA "prohibits intentionally accessing a computer without authorization or in excess of authorization", however, the law lacks definition of what "without authorization" addresses.

1987 - John McAfee created the first anti-virus software, primarily in response to the virus Brain, the first virus for MS-DOS.[12] McAfee initially made the software free to use for individual users, but charged companies a fee.[13] In 1989 he was able to leave his previous company and devote all his time to McAfee.[14] Today, McAfee still remains on the market as one of the best anti-virus softwares.

---

[6] Featherly, "ARPANET," Encyclopedia Britannica
[7] Kanade, "What Is ARPANET?," Spiceworks
[8] Chen and Robert, "The Evolution," 3
[9] Awati, "Elk Cloner," TechTarget
[10] Ibid
[11] "Computer Fraud," National Association of Criminal Defense Lawyers
[12] "Cybersecurity Profile," Cybersecurity Education Guides
[13] Ibid
[14] Ibid

1988 - In early November 1988, the Morris worm was unleashed onto the internet from a Massachusetts Institute of Technology (MIT) computer and attacked computers at major universities across the country, all of which used a Unix operating system.[15] The virus didn't damage or destroy files, however it slowed computers down significantly affecting emails, and vital university and military functions.[16] The Morris worm was the first large scale virus and is still looked back on almost 40 years later.

1989 - The first ransomware attack took place via a mailed floppy disk that said it would help determine if someone was at risk of developing AIDs.[17] Instead, after the 90th reboot, the program would hide directories and encrypt files, displaying a message requesting a check be sent to Panama if they wanted their computer to be unlocked.[18] Ransomware is a cybersecurity threat that still occurs to this day, setting people and companies back several thousand dollars.

1991 - The first website was launched, containing information regarding the WorldWideWeb (W3) project.[19] "It launched at the European Organization for Nuclear Research, CERN, where it was created by British computer scientist Tim Berners-Lee" and contained information for anyone on the internet to create their own website. [20] Today, there are millions of websites and W3 laid the foundation for most of what everyone around the world uses in their daily lives.

1993 - The first DEF CON security conference was held by Jeff Moss in Las Vegas and brought (and currently brings) together cybersecurity experts and people who just want to learn more about cybersecurity.[21] The conference is held to this day and has grown to be the largest cybersecurity conference in the world and continues to impact developments in the field.[22]

1998 - The Russian Federation proposes a United Nations (UN) treaty to limit the use of cyber weapons and cyber attacks.[23] As there was significant distrust between states at this time, the proposal went nowhere.[24] Despite not being successful at the time, this proposal laid the groundwork for a "2010 report of the second UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)".[25]

---

[15] United States Government, "The Morris," Federal Bureau of Investigation
[16] Ibid
[17] Browne, "Tech Ransomware," CNBC
[18] Ibid
[19] Fischels, "A Look," NPR
[20] Ibid
[21] Dalziel, "DEF CON," InfoSec
[22] Ibid
[23] Lewis, "Sustaining Progress," Centre for Strategic and International Studies
[24] Ibid
[25] Ibid

2000 - The ILOVEYOU bug was unleashed and within 24 hours, 45 million computers were infected and overall, approximately 10 per cent of all computers connected to the internet were impacted by the virus.[26] The virus spread via an email which upon opening the attached file, which appeared to be a love letter, would delete the recipient's files as well as send the email to everyone in their email contacts.[27] The virus itself caused billions of dollars in damages and to this day remains one of the most destructive.[28]

2001 - The Council of Europe Convention on Cybercrime, better known as the Budapest Convention and was ratified by 81 countries and a further 16 are signatories, invited to accede to the convention.[29] The convention itself "calls for the criminalization of certain offences relating to computers, the adoption of procedural powers for investigating and prosecuting cybercrime, and the promotion of international cooperation through mutual legal assistance and extradition in a criminal realm that knows no borders".[30] To this day, "the treaty is the only widely recognized attempt to deal with cybercrime issues and contains the most widely accepted typology of cybercrime".[31]

2004 - The first worm infecting mobile devices, the Cabir worm was released into the world and spread through bluetooth connections.[32] Additionally, it required users permission to download, making it entirely the users fault.[33] Once active, the worm would force the phone to display "Caribe" as well as search for other devices via bluetooth to spread the virus to.[34]

2007 - In late April, Estonia came under cyberattack heavily from the Russian federation (however Moscow continues to deny its involvement) with the goal of crippling the infrastructure of the state.[35] This was the first instance of a state-sponsored cyberattack, however far from the last.[36]

2010 - The Stuxnet worm attacked a nuclear facility in Iran and "reportedly destroyed numerous centrifuges in Iran's Natanz uranium enrichment facility by causing them to burn themselves out".[37] It appeared to have been created by the "U.S. National Security Agency, the CIA, and Israeli intelligence" and was the first computer worm capable of physical destruction.[38]

---

[26] Spivack, "'ILOVEYOU': How the Infamous," History
[27] Ibid
[28] Ibid
[29] "Backgrounder - Council," Government of Canada; Council of Europe, "The Convention," Cybercrime
[30] "Backgrounder - Council," Government of Canada
[31] Ibid
[32] Editor, "A history," welivesecurity
[33] Ibid
[34] Ibid
[35] MacLellan and O'Leary, "Doing Battle," Centre for International Governance Innovation
[36] Ibid
[37] "What Is Stuxnet?," Trellix
[38] Ibid

2018 - Introduced in 2018, “the General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world” and “imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU”.[39] If regulations are violated, offenders can face fines up to tens of millions of euros.

2020 - After the outbreak of COVID-19, most of the world went online for work, increasing potential targets for cyberattacks and malicious malware. Additionally weakened security systems due system overload resulted in information leaks, stolen intellectual property, and a surge in digital fraud.[40] However, to combat this issue cybersecurity companies made advancements in their software and people became more aware of the risks of being online.

2022 - Costa Rica becomes the first state to declare a state of emergency as a result of cyberattacks from a Russian-speaking gang, the Conti[41]. At the time of declaration, the Conti had been attacking the Costa Rican government for two years and ransoms totalling 150 million dollars and impacting around 1,000 Costa Ricans.[42]

2025 - With the rise of AI, deepfakes and increased use have allowed many people with no previous knowledge, the ability to create code to launch cyberattacks along with targeting less internet informed groups such as the elderly. However, AI can also help companies develop new cybersecurity technologies and provide greater access to internet knowledge with its ability to adapt to the user.

Past International Involvement

The Budapest Convention

The Budapest Conventions, officially named the Convention on Cybercrime of the Council of Europe w as adopted in 2001. This framework was established as the first of its kind to address crimes committed on the internet, particularly crimes related to computer-related forgery and fraud, violations of network security, and copyright infringement.[43] Since 2001, there have been two additional protocols added to the convention. The first protocol defines racist and xenophobic actions conducted online as criminal, while the second was created to improve protections for internet users and facilitate better responses for victims of digital crimes.[44] Though the convention has faced some criticism since its enactment, it is currently one of the most well regarded and successful policies in the area of cybercrimes. This is due in part to its incorporation of human rights safeguards and widespread ratification across four continents,

[39] Wolford, "What is GDPR," GDPR.EU
[40] DST, "Pandemic and Cyber," Kymatio
[41] AP in San Jose, "Costa Rica," The Guardian
[42] Ibid
[43] Convention on Cybercrime, [Page 5-7]
[44] Zachar, "Battling Cybercrime," Cooperative Cyber Defence Centre of Excellence

which gives it international backing and recognition.[45] Currently, around 80% of nations worldwide use it as a guideline or source of inspiration in domestic legislation regarding cybercrime.[46]

ITU Global Cybersecurity Agenda (GCA)

Established in 2007, the GCA creates a system to facilitate global collaboration in cybersecurity.[47] The International Telecommunications Union (ITU) responsible for the creation of this framework, and the UN's specialty agency for information and communications technologies. This agenda was "designed to encourage collaboration and build on existing initiatives".[48] This plan, while not terribly influential on the world stage, has laid a strong path on which other policies and initiatives have relied on.

United Nations Cybersecurity & New Tech Programme

The UN Cybersecurity and New Technology Programme led by the UN Office of Counter-Terrorism (UNOCT) has had a significant impact in education around cybercrimes since its inception in April of 2020. It has reached and/or trained over 4500 individuals, 1400 of those being women.[49] This program aims to teach officials in Member states how to investigate and counter cybercrime terrorists, as well as "building a collective understanding on the threat of malicious uses of new technologies by terrorists".[50] This has been an excellent resource in ensuring nations are knowledgeable about appropriate responses regarding cybercrimes.

United Nations Convention Against Cybercrime

The United Nations Convention Against Cybercrime was adopted in December of 2024, though it is not yet entirely ratified.[51] The convention is based largely on the Budapest Conventions, with some notable differences. It aims to improve protocols to combat cybercrimes efficiently, promote technical assistance and capacity building for cybercrimes, and facilitate cooperation between countries in preventing and reacting to cybercrimes.[52] While many see this convention as an important step in the right direction, there are also some critics of it. Citing its wording and policies regarding the unlimited prosecution power it grants states for cybercrime criminals, some say there are risks of possible abuse and overreach of the policies, especially by

[45] Marcén, "The Budapest," [Page 176-177]
[46] "The global," Council of Europe
[47] "Global Cybersecurity," International Telecommunications Union
[48] "Keeping pace," International Telecommunication Union
[49] "Cybersecurity and New Technologies," United Nations Office of Counter-Terrorism
[50] "Home About," UNOCT
[51] "United Nations," United Nations Office on Drugs and Crime
[52] "United Nations," Sirius

authoritarian regimes.[53] In particular, there are concerns that human rights activists and journalists could be at risk should they publish work online that is critical of actions or policies of a government. Said government could then label it as a cybercrime, which would allow them substantial prosecuting power according to the convention.[54] Seeing as the convention has not yet been ratified, the long term impacts of this convention are not yet known.

Current Situation

Variety in Cybercrime

The types of cybercrime are exceptionally varied, though some are more common than others. These include malware and ransomware attacks, phishing, identity theft, cyberstalking, and cyberterrorism.[55] A range of tactics are used to conduct such crimes, including network intrusion, malware distribution, and social engineering. These crimes are threats to individuals, institutions, and nations around the world, and the response to each type of cybercrime requires different skills.[56]

Due to this variety, responses can be quite mixed. International organizations, like INTERPOL, commonly work to combat cybercrimes by disrupting the activities of cybercriminals and prioritizing communities and building capacity for response to possible cyber crimes.[57] States' governments, in comparison, typically place their first priority in the protection of their people and country before international standards.[58] Nevertheless, these two groups' actions are more often than not linked.

The network of criminals committing these crimes are also linked. "Numerous interconnected but independent criminals utilize a wide variety of internet-based crimes to exploit opportunities," which means that even when the individual responsible for one crime is caught, another will inevitably fill the space.[59]

Impact of Artificial Intelligence

The rapid development of artificial intelligence (AI) has lasting implications in the world of cybersecurity. In this new era, cybercrimes enabled by AI are becoming a reality.
In 2024, an employee of the engineering company Arup conducted a routine transfer of millions of dollars after a video conference with some members of senior management. As it turns out, however, the video call had been an AI deepfake, and the fraudsters managed to steal $25 million USD.[60] Like in this example, artificial intelligence has been used to imitate humans. Whether by

[53] Tennant, "UN cybercrime," Global Initiative Against Transnational Organized Crime; Bannelier, "Risks and Opportunities," [Page 1, 11-12]; Benítez-Mongelós, "The UN Cybercrime," Global Campus on Human Rights
[54] Benítez-Mongelós, "The UN Cybercrime," Global Campus on Human Rights
[55] Loux, "Types of Cybercrime," American Military University
[56] Rehman et al., "Varieties and Skills," [Page 2]
[57] "Cybercrime – our response," INTERPOL
[58] "Cyber Security," Public Safety Canada
[59] Sigursteinsson, "The complexity," Dalhousie University
[60] Elliott, "'This happens," World Economic Forum

creating fake videos or cloning the voices of loved ones, these scams have proven to be hard to detect, especially for vulnerable individuals. These scams are a form of phishing, which is a type of cybercrime involving imitating legitimate individuals or institutions for the purpose of extracting money and/or sensitive information from them.[61]

The widespread access to artificial intelligence is also lowering the barriers to cybercrime. Individuals already involved in other types of crime now have a much easier time transitioning into cybercrime. Those who had previously been deterred by the technical skills needed to commit cybercrimes are now also more likely to choose AI aided tactics.[62] Although AI is not quite yet capable of creating highly sophisticated malware on par with the elite programs of today, there are continual improvements in this area, and it may be a reality in the not so distant future.[63]

Possible Solutions and Controversies

AI Governance & Regulation

As artificial intelligence (AI) continues to grow at alarming rates, the risk of autonomous attacks on digital infrastructure grows as well with new technology and AI progress threatening the online safety of many. Bearing this in mind, a possible solution presents itself through this issue, this being the governance, surveillance, and regulation of AI application and software. Stated on the Centre for Strategic and International Studies (CSIS), it is said that; “On September 25, the United Nations launched the Global Dialogue on AI Governance. The dialogue aims to provide a platform for future discussions of AI governance. Governments and other stakeholders will convene annually—starting at the 2026 AI for Good Global Summit in Geneva—to discuss the safe development of AI systems, AI capacity gaps in developing countries, interoperability of national AI governance efforts, and socioeconomic implications of AI technologies”.[64] The solution presented would prove effective as it both calls for states to cooperate and gives a foundation to work up, allowing nations to share their information and ideas while having a general framework to work with.

Strengthening Global Infrastructure Security - Case Study: European Parliament Directive

Acknowledging that threats to digital infrastructure will persist with new ones showing themselves as time continues, the strengthening of said infrastructure is of utmost importance. A good example for a solution to this would be the Directive on the Resilience of Critical Entities adopted by the European Parliament in 2022. The Directive aimed to strengthen the resilience of critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies.[65]

---

[61] Huang, "The Anatomy," Group-IB
[62] Manky and Baram, "Beyond Phishing," Center for Long-Term Cybersecurity
[63] "How artificial," Control Risks
[64] Caroli and Mande, "What the UN Global," Centre for Strategic and International Studies
[65] "Critical infrastructure," European Commission

Under the new rules, Member States were required to adopt a national strategy and carry out regular risk assessments to identify entities that are considered critical or vital for society and the economy.[66] Risk assessments were to be carried out as regards to these essential services, so that critical entities in each member state can be identified. In turn, the critical entities were required to carry out risk assessments of their own and take technical, security and organisational measures to enhance their resilience and notify incidents.[67] Another rule stated that; Critical entities in the EU providing essential services in six or more Member States were to benefit from extra advice on how best to meet their obligations to assess risks and take resilience-enhancing measures.[68] The Commission would also provide complementary support to Member States and critical entities, by developing a Union-level overview of cross-border and cross-sectoral risks, best practices, guidance material, methodologies, cross-border training activities and exercises to test the resilience of critical entities, among others.[69]

The Critical Entities Resilience Group (CERG), was established by the Directive and facilitates cooperation among Member States and within the European Commission.[70] It allows for exchange of information and good practices on issues relating to the resilience of critical infrastructure and of critical entities. The group is chaired by the Commission and consists of representatives of competent authorities in Member States.[71]

The Directive covered the following eleven sectors: Energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, space, production, processing and distribution of food, allowing it to benefit multiple areas that reach out from DISEC.[72] Adopting a similar resolution in this committee would bring the opportunity for solutions to support outside issues and topics if not fully solving them.

The main controversy would be the restrictive and implicit cooperative nature of the resolution, making it unappealing to isolationist states.

Increasing Data Accessibility

With technology getting better by the day, corporations are given more room to move around when it comes to taking and selling the data of people using their websites. Some believe that making data more accessible in the same way that cybercriminals do will keep businesses a step ahead.[73] As infiltrations become more prolific, coordinated and commoditised, organisations can't afford to let cybersecurity skills gaps or outdated defence strategies hamper their responses as "the attack surface has become way bigger".[74] There are three major problems that

[66] "Critical infrastructure," European Commission
[67] Ibid
[68] Ibid
[69] Ibid
[70] Ibid
[71] Ibid
[72] Ibid
[73] "Open warfare," Raconteur
[74] Ibid

cybersecurity defensive teams face, speed of digital transformation, growth of nation-state attacks, and talent scarcity.[75] The speed of digital transformation post-pandemic, which opened up holes due to businesses "accelerated transition to the cloud".[76] Finally, talent scarcity in the security space which makes it harder for individual teams to keep up with new and emerging threats. Working together to achieve the common goal of " mak[ing] the adversary work harder" is perhaps the best way of dealing with an evolving cybersecurity field, ensuring the safety of data and infrastructure.[77] However, it is also clear that this idea does not appeal to all states as some wish to be less forward about their information with many companies sharing this same moral.

Bloc Positions

Data Regulation Bloc

The Data regulation bloc would consist of Europe and member states of the GDPR (mentioned in the timeline section). This bloc would push for more restrictive policies on data usage globally along with expanding the GDPR worldwide, protecting citizen data around the world.[78] This bloc does not use cybersecurity as an excuse for censorship such as members of the censorship bloc. The most likely allies for this bloc would be the Middle ground and/or the National security bloc as they would agree on some policies.

Middle Ground Bloc

The Middle Ground consists primarily of Australia, New Zealand, India, and Turkiye to name a few and combine the national security interests of the National Security bloc along with the strict data protection laws of the Data protection bloc. Sometimes known for making their own way such as India's desire to not rely on foreign aid, this bloc can help bridge the gap between the National Security and Data Protection blocs, more specifically the US, and these blocs are where the Middle Ground bloc would find their allies.

National Security Bloc

The open bloc primary consists of the United States, Japan, and South Korea and is focused on national security. While some policies on data regulations may differ, such as the US collaborating with a lot of tech corporations which allows for the free flow of data while Japan may focus more on data protection, but both still have national interests in mind.[79] The most likely allies for this bloc would be the middle ground and/or European bloc as they would agree on some policies.

---

[75] "Open warfare," Raconteur
[76] Ibid
[77] Ibid
[78] Musoni et al., "Global Approaches," [Page 10]
[79] Ibid

Censorship Bloc

The censorship bloc primarily consists of Russia, China, and Iran who use cybersecurity as an excuse or justification to censor information presented to their citizens. While some policies may align with those in the data regulation bloc in that they have strict data policies, these countries do not align politically with EU members and would differ greatly on how to implement policies.[80] This bloc would not find many Allies, however they could form alliances with the promise of aid to the Developing Countries bloc.

Developing countries

The Developing Countries bloc consists of countries like those situated in Africa, or South/Latin America that may not have the same policies or infrastructure in place as the other blocs. Most countries vary on their stance on cybersecurity and data policy and may require aid from other blocs.[81] Depending on the country, they may or may not accept foreign aid from other blocs, but if interested in forming alliances for resolution papers, they may need to make concessions while maintaining country policy.

Discussion Questions

1. How can countries effectively balance human rights and freedom of speech with cybersecurity?
2. How can countries work together to eliminate the threats of cyberattacks?
3. How does international cybersecurity legislation present a threat to national sovereignty?
4. What steps can the UN take to protect critical infrastructure against cyber attacks?
5. How can the UN ensure that countries responsible for cyberattacks are held accountable?
6. What can be done to prevent countries from using cybersecurity laws as an excuse to censor media?
7. How can the discussion incorporate the views of small or developing countries?
8. How does the rise of AI change the way defense against cyberattacks takes place?
9. What measures can be adopted to educate the youth and elderly to be aware of scams and potential cyberattacks
10. How can countries and companies limit the amount of time it takes to identify and resolve a cybersecurity threat?

[80] Musoni et al., "Global Approaches," [Page 10]
[81] Ibid

Works Cited

AP in San Jose. "Costa Rica declares national emergency amid ransomware attacks." The Guardian. Last modified May 12, 2022. Accessed February 12, 2026. https://www.theguardian.com/world/2022/may/12/costa-rica-national-emergency-ransomware-attacks.

Awati, Rahul. "Elk Cloner." TechTarget. Last modified December 8, 2021. Accessed February 6, 2026. https://www.techtarget.com/searchsecurity/definition/Elk-Cloner.

"Backgrounder - Council of Europe Convention on Cybercrime." Government of Canada. Last modified December 14, 2016. Accessed February 10, 2026. https://www.canada.ca/en/news/archive/2015/07/backgrounder-council-europe-convention-cybercrime.html.

Bannelier, Karine. "Risks and Opportunities of the UN Cybercrime Convention for the UNDOC & The Fight against Transnational Organised Crime: A First Assessment." *Transnational Criminal Law Review* 4, no. 1 (2025). https://doi.org/10.22329/tclr.v4i1.9468.

Barbier, Joeri. "Cyberwar, Sanctions & Sovereignty – When Geopolitics Becomes a Security Gap." Getronics. Last modified November 17, 2025. Accessed February 9, 2026. https://www.getronics.com/cyberwar-sanctions-sovereignty-when-geopolitics-becomes-a-security-gap/.

Benítez-Mongelós, Sara. "The UN Cybercrime Convention: why it endangers human rights defenders and journalists." Global Campus on Human Rights. Last modified March 13, 2025. Accessed February 12, 2026. https://www.gchumanrights.org/preparedness/the-un-cybercrime-convention-why-it-endangers-human-rights-defenders-and-journalists/.

Browne, Ryan. "Tech Ransomware is 35 years old and now a billion-dollar problem. Here's how it could evolve." CNBC. Last modified December 30, 2024. Accessed February 10, 2026. https://www.cnbc.com/2024/12/30/ransomware-35-years-on-history-behind-hacking-method-and-whats-next.html.

Can, Muhammed. "Grey Zone Conflicts in Cyber Domain." Abstract. *Encyclopedia of Criminal Activities and the Deep Web*, 2020, 271-86. https://doi.org/10.4018/978-1-5225-9715-5.ch018.

Caroli, Laura, and Matt Mande. "What the UN Global Dialogue on AI Governance Reveals About Global Power Shifts." Centre for Strategic and International Studies. Last modified October 7, 2025. Accessed February 9, 2026. https://www.csis.org/analysis/what-un-global-dialogue-ai-governance-reveals-about-global-power-shifts.

Chen, Thomas M., and Jean-Marc Robert. "The Evolution of Viruses and Worms." In *Statistical Methods in Computer Security*, edited by William W.S. Chen. CRC Press, 2004. https://doi.org/10.1201/9781420030884.

"Computer Fraud and Abuse Act (CFAA)." National Association of Criminal Defense Lawyers. Accessed February 9, 2026. https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

Convention on Cybercrime = Convention Sur La Cybercriminalité ; Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems = Protocole Additionnel À La Convention Sur La Cybercriminalité, Relatif À L'incrimination D'actes De Nature Raciste Et Xénophobe Commis Par Le Biais De Systèmes Informatiques. 2001.

Council of Europe. "The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols." Cybercrime. Accessed February 10, 2026. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

"Critical infrastructure resilience at EU-level." European Commission. Last modified January 13, 2026. Accessed February 9, 2026. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en?

"Cybercrime – our response." INTERPOL. Accessed February 12, 2026. https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-our-response.

"Cybersecurity Profile: John McAfee, Godfather of Antivirus Software." Cybersecurity Education Guides. Accessed February 10, 2026. https://www.cybersecurityeducationguides.org/john-mcafee-godfather-of-antivirus-software/.

Dalziel, Henry. "DEF CON: The Iconic Hacker Conference." InfoSec. Accessed February 10, 2026. https://infosec-conferences.com/hub/event-series/def-con.

"Data Breaches 2025: Biggest Cybersecurity Incidents So Far." *PKWARE* (blog), January 2, 2026. Accessed February 9, 2026. https://www.pkware.com/blog/recent-data-breaches.

DST. "Pandemic and Cyber risk, incidence of COVID-19 in cybersecurity." Kymatio. Last modified March 17, 2020. Accessed February 12, 2026. http://kymatio.com/blog/pandemic-incidence-of-covid19-in-cybersecurity.

Editor. "A history of mobile malware from Cabir to SMS Thief." welivesecurity. Last modified November 1, 2016. Accessed February 11, 2026. https://www.welivesecurity.com/2016/11/01/history-mobile-malware-cabir-sms-thief/.

Elliott, David. "'This happens more frequently than people realize': Arup chief on the lessons learned from a $25m deepfake crime." World Economic Forum. Last modified February

4, 2025. Accessed February 12, 2026. https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/.

European Union Agency for Criminal Justice Cooperation. "United Nations Convention Against Cybercrime." Sirius. Last modified July 4, 2021. Accessed February 12, 2026. https://www.eurojust.europa.eu/publication/united-nations-convention-against-cybercrime.

Featherly, Kevin. "ARPANET." Encyclopedia Britannica. Last modified January 28, 2026. Accessed February 9, 2026. https://www.britannica.com/topic/ARPANET.

Fischels, Josie. "A Look Back at the Very First Website Ever Launched, 30 Years Later." NPR. Last modified August 6, 2021. https://www.npr.org/2021/08/06/1025554426/a-look-back-at-the-very-first-website-ever-launched-30-years-later.

Fleming, Sean. "What is digital sovereignty and how are countries approaching it?" World Economic Forum. Last modified January 10, 2025. Accessed February 12, 2026. https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/.

"Global Cybersecurity Agenda (GCA)." International Telecommunications Union. Accessed February 10, 2026. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx.

"The global state of cybercrime legislation 2013 – 2021: A cursory overview." Council of Europe. Last modified June 30, 2021.

Government of Canada. "Cyber Security in the Canadian Federal Government." Public Safety Canada. Last modified December 13, 2024. Accessed February 12, 2026. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/fdrl-gvrnmnt-en.aspx.

"Home About FAQ Contact us Go to Connect Log in Cybersecurity & New Technologies." UNOCT. Accessed February 12, 2026. https://learn.unoct-connectandlearn.org/course/index.php?categoryid=26.

"How artificial intelligence is lowering the barrier to cybercrime." Control Risks. Last modified October 30, 2024. Accessed February 12, 2026. https://www.controlrisks.com/our-thinking/insights/how-artificial-intelligence-is-lowering-the-barrier-to-cybercrime.

Huang, Yuan. "The Anatomy of a Deepfake Voice Phishing Attack: How AI-Generated Voices Are Powering the Next Wave of Scams." Group-IB. Last modified August 6, 2025. Accessed February 12, 2026. https://www.group-ib.com/blog/voice-deepfake-scams/.

Kanade, Vijay. "What Is ARPANET? Definition, Features, and Importance." Spiceworks. Last modified July 5, 2023. Accessed February 9, 2026. https://www.spiceworks.com/networking/what-is-arpanet/.

"Keeping pace: ITU's Global Cybersecurity Agenda." International Telecommunication Union. Last modified March 9, 2021. Accessed February 12, 2026. https://www.itu.int/hub/2021/03/keeping-pace-itus-global-cybersecurity-agenda/.

Lee, Timothee B., and Emily St. James. "The 2014 Sony hacks, explained." Vox. Last modified June 3, 2015. Accessed February 6, 2026. https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea.

Lewis, James Andrew. "Sustaining Progress in International Negotiations on Cybersecurity." Centre for Strategic and International Studies. Last modified July 25, 2017. Accessed February 10, 2026. https://www.csis.org/analysis/sustaining-progress-international-negotiations-cybersecurity.

Lindemulder, Gregg. "What is cybersecurity?" Edited by Matthew Kosinski and Alexandra Jonker. IBM. Accessed February 5, 2026. https://www.ibm.com/think/topics/cybersecurity.

Loux, Matthew. "Types of Cybercrime and Different Cyber Warfare Tactics." American Military University. Last modified July 29, 2025. Accessed February 12, 2026. https://www.amu.apus.edu/area-of-study/criminal-justice/resources/types-of-cybercrime/.

MacLellan, Stephanie, and Naomi O'Leary. "Doing Battle in Cyberspace: How an Attack on Estonia Changed the Rules of the Game." Centre for International Governance Innovation. Last modified October 26, 2017. Accessed February 11, 2026. https://www.cigionline.org/articles/doing-battle-cyberspace-how-attack-estonia-changed-rules-game/.

Manky, Derek, and Gil Baram. "Beyond Phishing: Exploring the Rise of AI-enabled Cybercrime." Center for Long-Term Cybersecurity. UC Berkely. Last modified January 2025. Accessed February 12, 2026. https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime/.

Marcén, Ana Gascón. "The Budapest Convention and the UN Cybercrime Convention Negotiations." *Global Cybersecurity and International Law*, March 27, 2024, 174-92. https://doi.org/10.4324/9781003344124-10.

Musoni, Melody, Poorva Karkare, Chloe Teevan, and Ennatu Domingo. "Global Approaches to Digital Sovereignty: Competing Definitions and Policies." *European Centre for Development Policy Management*, May 2023. Accessed February 12, 2026. https://coilink.org/20.500.12592/8fg3m4.

Nason, Alanna. "A History of Cybersecurity and Cyber Threats." Coro. Last modified April 25, 2024. Accessed February 6, 2026. https://www.coro.net/blog/history-of-cybersecurity-and-cyber-threats.

"Open warfare: will data-sharing win the fight against cybercriminals?" Raconteur. Accessed February 11, 2026. https://www.raconteur.net/risk-regulation/will-data-sharing-win-the-fight-against-cybercriminals.

"Recent Breaches." Breachsense. Accessed February 9, 2026. https://www.breachsense.com/breaches/.

Rehman, Tansif Ur, Sajida Parveen, Mehmood Ahmed Usmani, and Muhammad Ahad Yar Khan. "Varieties and Skills of Cybercrime." *International Journal of Cyber Behavior, Psychology and Learning* 13, no. 1 (2023): 1-13. https://doi.org/10.4018/ijcbpl.324091.

Sigursteinsson, Bjarni. "The complexity of cybercrime." Dalhousie University. Last modified December 14, 2021. Accessed February 12, 2026. https://blogs.dal.ca/openthink/the-complexity-of-cybercrime/.

Spivack, Elana. "'ILOVEYOU': How the Infamous Computer Worm Wreaked Havoc." History. A&E Television Networks. Last modified May 8, 2025. https://www.history.com/articles/i-love-you-computer-worm.

Tennant, Ian. "UN cybercrime convention." Global Initiative Against Transnational Organized Crime. Last modified November 18, 2025. Accessed February 12, 2026. https://globalinitiative.net/analysis/a-conference-of-contradictions-in-hanoi/.

United Nations. "Cybersecurity and New Technologies." United Nations Office of Counter-Terrorism. Accessed February 12, 2026. https://www.un.org/counterterrorism/en/cct/programme-projects/cybersecurity.

United Nations. "United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes." United Nations Office on Drugs and Crime. Accessed February 12, 2026. https://www.unodc.org/unodc/en/cybercrime/convention/home.html.

United States Government. "The Morris Worm." Federal Bureau of Investigation. Last modified November 2, 2018. Accessed February 10, 2026. https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.

"What Is Stuxnet?" Trellix. Accessed February 11, 2026. https://www.trellix.com/en-ca/security-awareness/ransomware/what-is-stuxnet/.

Wolford, Ben. "What is GDPR, the EU's new data protection law?" GDPR.EU. Accessed February 11, 2026. https://gdpr.eu/what-is-gdpr/.

Zachar, Dominik. "Battling Cybercrime Through the New Additional Protocol to the Budapest Convention." Cooperative Cyber Defence Centre of Excellence. Accessed February 12,

2026.
https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/.