Special Political and Deconolization Committee

Foreign Technological Interference and Its Threat to Political Self-Determination

Backgrounder Guide

Table of Contents

Director's Letter

Dear Delegates,

Welcome to the Special Political and Decolonization Committee (SPECPOL) at the 2025 iteration of SPAMUN! My name is Allen Wang, and I am beyond thrilled to serve as your Director alongside my Chair, Sandro Wang and my Assistant Director, Zoe Lheritier. On behalf of the entire Dais team, I'd like to issue a warm welcome to everyone and look forward to working towards our mission to foster sophisticated yet fruitful debates, giving all delegates, no matter whether it's your first or tenth conference, the best possible experience. I eagerly await meeting all of you in October and hope each and every one of you will have unforgettable experiences at SPAMUN 2025.

This iteration, SPECPOL will be addressing one of the most pressing challenges that has come up in the 21st century: The use of technology as a tool for foreign interference used against sovereign nations to influence their political processes. The constant yet rapid expansion of the internet, popularization of social media platforms and development of advanced surveillance technologies have opened new avenues for foreign state and non-state actors to influence, destabilize, or manipulate political systems abroad internationally.

Our task in this committee will be to examine the legal, political and ethical challenges of such interference, to balance national sovereignty with international cooperation. You will need to understand the nature of these threats as well as the complex background rivalries that drive them. Ultimately, the goal is to determine how nations can safeguard their political sovereignty without isolating themselves from global collaboration.

To determine a nation's ability to manage its own political sovereignty without external interference. We strongly encourage all delegates to approach this topic with open-minded, solution-oriented perspectives. If you have any questions, feel free to reach out to us using our committee email address at specpolspamun@southpointe.ca. Position papers are due on October 7 for feedback, and on October 14 for final submission.

Sincerely,
Allen Wang

Committee Description

The Special Political and Decolonization Committee (SPECPOL), also known as the Fourth Committee of the UN General Assembly, is one of the six central committees in the United Nations. Originally founded in 1993, SPECPOL was formally established to fulfill the United Nations mission for eradicating colonialism, from the 20th-21st centuries. Throughout the aftermath of World War II, SPECPOL aided various territories' transitions from colonized regions to independent nations. When the United Nations was first established in 1945, over 700 million people — almost a third of the world's population lived in colonized territories. In contrast, as of today, the number of people living in colonized territories stands at an all-time low of two million, proving the success under the mandate of SPECPOL.

Present day, SPECPOL works towards decolonization, peacekeeping, and humanitarianism issues. Some of which include Palestinian refugees, governance of outer space technologies, and political sovereignty. SPECPOL's resolutions are non-binding and cannot enforce binding resolutions, such as issuing international sanctions. However, SPECPOL can recommend guidelines for independent nations to adopt voluntarily.

Topic Overview

Foreign technological interference occurs when foreign state or non-state actors influence, disrupt, or manipulate another independent country's political independence with the use of digital tools. Cyberattacks on elections, targeted political organization hacking, and the dissemination of false material via social media to support political narratives are just a few examples of this. Foreign actors can now influence public opinion or topple entire political systems from thousands of miles away thanks to the internet and online platforms, which have made these operations faster, easier, and more difficult for authorities to track down, particularly in recent years. This problem challenges the idea of political sovereignty, which holds that countries should be able to make their own decisions without interference from outside parties.

Over the past decade, numerous countries have reported incidents of foreign technological interference. In 2016, the United States accused Russia of sending foreign actors to hack into private political party emails and spreading political propaganda campaigns during their presidential elections. In 2017, French authorities accused Russian-linked hackers of leaking presidential candidate

Emmanuel Macron's campaign emails just days before voting, aiming to negatively impact his chances. Even smaller nations like the Democratic Republic of the Congo have experienced interference: Their 2018 elections were ridiculed online by misinformation on platforms such as Facebook and WhatsApp.

While it is more common that democratic countries are in the position to accuse authoritarian states of foreign technological interference, history has proven that accusations also run in the opposite direction. The United States, for instance, has faced constant criticism for its own digital interference. The 2013 Snowden leaks revealed that the U.S. National Security Agency (NSA) was conducting surveillance on foreign leaders and governments, even including U.S. allies such as Germany and Brazil. Similarly, the UK-based firm Cambridge Analytica was linked to multiple cases of election manipulation and disinformation campaigns in Africa, Latin America, and Asia.

Given the possibility of eroding public confidence, toppling governments, and even intensifying tensions amongst geopolitical actors, foreign technological involvement must be addressed. This problem is a worldwide crisis with a breadth that extends far beyond the nations mentioned above. Although developing countries, growing industrialized nations, and wealthy democracies are all impacted, smaller governments are frequently the most vulnerable because of poverty and government corruption, which, as a result, weakens cybersecurity mechanisms. Furthermore, the effects of foreign technical meddling go well beyond just governments, as non-governmental organizations (NGOs) have their efforts undermined by fake disinformation.

Timeline of Events

June 5, 2013 — Former NSA contractor Edward Snowden leaks classified information exposing the United States' extensive global surveillance programs, including PRISM and FISA. Documents show the NSA monitored emails, phone calls, and internet activity of both foreign citizens and allied leaders such as Germany's Angela Merkel and Brazil's Dilma Rousseff.

March 19, 2014 — During the Ukraine crisis, Russian state-linked hackers deploy cyberattacks and disinformation campaigns to destabilize Ukraine's government and support the annexation of Crimea.

June 4, 2015 — The U.S. Office of Personnel Management reports a major data breach compromising the personal information of 21 million federal employees. The attack is widely attributed to Chinese state-linked actors.

November 8, 2016 — The U.S. presidential election is marred by allegations of Russian interference, including the hacking of Democratic Party emails and large-scale social media disinformation campaigns aimed at influencing voter opinion.

May 5, 2017 — Just two days before France's presidential election, Russian-linked hackers leaked thousands of Emmanuel Macron's campaign emails in an attempt to sway voters.

August 8, 2017 — Investigations reveal that Cambridge Analytica, a UK-based political consulting firm, harvested millions of Facebook profiles without consent to influence elections, including in Kenya's 2017 general election.

December 30, 2018 — The Democratic Republic of the Congo's elections are heavily targeted by online disinformation, with false reports about voting fraud and violence circulating on Facebook and WhatsApp, allegedly amplified by foreign-based accounts.

February 8, 2019 — The Australian Parliament suffers a cyber breach targeting major political parties. Chinese state-linked hackers are suspected to be responsible.

January 11, 2020 — Taiwanese officials accuse China of orchestrating coordinated social media disinformation campaigns against pro-independence candidates in Taiwan's presidential election.

October 21, 2020 — U.S. intelligence warns that Russia, Iran, and China are attempting to interfere in the 2020 U.S. elections through hacking operations and online propaganda.

March 2, 2021 — A massive hack exploiting Microsoft Exchange vulnerabilities compromises tens of thousands of organizations worldwide. The attack is attributed to Chinese state-linked hackers.

February 24, 2022 — Following the invasion of Ukraine, Russia launches a surge of disinformation on social media platforms to justify its actions and undermine international support for Ukraine.

May 23, 2023 — Reports allege Chinese hackers targeted Kenya's Ministry of Foreign Affairs to monitor debt negotiations tied to Belt and Road Initiative projects.

July 17, 2023 — U.S. Cyber Command confirms it disrupted Russian troll farms ahead of allied elections, aiming to prevent disinformation campaigns targeting European allies.

July 2025 — Beijing denies espionage allegations from Australia, countering that Australian intelligence agencies themselves engaged in spying.

Historical Analysis

Historically, nations exerted control and influence through spying, propaganda and sabotage. However, in the early 1980s, the rise of digital technologies introduced new strategies of interference that fundamentally changed international relations. For the past 2 decades, technology, the internet, surveillance systems, and cyber warfare have become central tools of foreign political interference. As these technologies continue to evolve, foreign digital interference is becoming sophisticated and adaptive, making it increasingly difficult to detect, prevent and defend against.

https://medium.com/threat-intel/cyber-espionage-spying-409416c794ec

In the early 2000s, cyber espionage emerged as a dominant form of foreign political interference during the development stage of the modern computer. Governments and intelligence agencies would rely on data breaching software, malware, and even phishing attacks for lethal information from rival nations. Due to the limited cybersecurity and weak data protection at the time, cyber espionage was widespread. One of the notable cases was Moonlight Maze, being the most severe and longest-running cyber espionage case in world history. As a result, the government of Russia's operations stole a vast amount of classified information, documents, and codes.

https://www.sciencedirect.com/topics/computer-science/moonlight-maze

The first social media platform was created in 1980, but it was not until 2010 that social media and information warfare bloomed. The invention of X (Twitter), YouTube and Facebook gained popularity, and it opened doors for foreign actors. The strategies most used are disinformation campaigns, bot networks, troll farms and targeted advertising. In 2016, the Russian government operatives conducted foreign interference in the United States presidential elections. The interference was set for the victory of candidate Donald Trump by promoting and boosting his campaign. The Russian internet research agency created millions of troll farms on social media applications that spread disinformation about candidate Hilary Clinton. The foreign political interference strategies had a strong impact on U.S citizens, leading to the success of President Donald Trump in the presidential election in 2016.

https://www.npr.org/2020/08/18/903616315/senate-releases-final-report-on-russias-interference-in-2016-election

In 2020, foreign interference tactics became more advanced and dangerous because of the rise of artificial intelligence. Deepfakes are AI-generated hyper-realistic digital images able to change our perception of our world. Humans have few ways to determine deepfakes, some being audio calls that mimic people's voices or video personas. The algorithmic manipulation exploits technology programmes efficiently and quickly, making deepfakes hard to catch. During the U.S presidential election in 2016 and 2020, deepfake videos of Kim Jong Un and Vladimir Putin were created. The foreign interference deepfakes warned U.S. citizens to save the election, implying that they should abstain from voting for President Donald Trump. The activist responsible for the deepfake aimed to send her message across the United States, having politicians state the note, which brought attention to the matter. The U.S has responded 2 times by cancelling news outlets and channels, to stop the advertisement of the deepfake.

https://shotkit.com/ai-deepfakes-risks/

https://www.dailydot.com/news/putin-kim-jong-un-election-deepfakes/

Immediately, we are facing a crisis in warfare, having state-sponsored cyber operations interfering with political independence worldwide. Foreign interference is a key factor in hybrid warfare, gaining knowledge of military information or cyber tactics. This heavily disrupts the political states of countries, affecting election infrastructure, leaking obtained information and influencing media outlets. Countries like the Democratic Republic of Congo are preparing for the 2026 pre-election to prevent disinformation and foreign political interference from Rwanda, experienced since the independence of the DRC. The European Union aims to empower Congolese journalists during the election, using round-table tactics to beat media disinformation and manipulation.

https://eng.fatshimetrie.org/2023/10/20/information-manipulation-and-foreign-interference-how-congolese-journalists-are-preparing-for-the-presidential-elections/

Current Situation

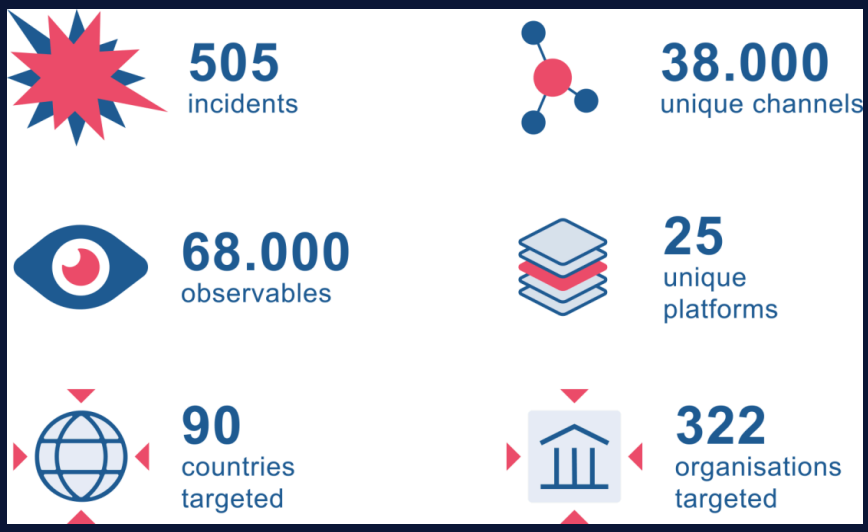
Today, there is a rapid growth of technological advancement and dependency worldwide. Through expansions of artificial intelligence, cloud computing and automation. Society is increasingly interconnected with technologies in our everyday lives, making the programmes more complex to comply with our rapid evolution. Technological advancement benefits the economic development of countries, industries, technologies and decision-making. Allowing indirect management of daily tasks or larger jobs, diminishing expenses. In addition, the government and corporate surveillance on the population, to ensure the security or manipulation of the citizens.

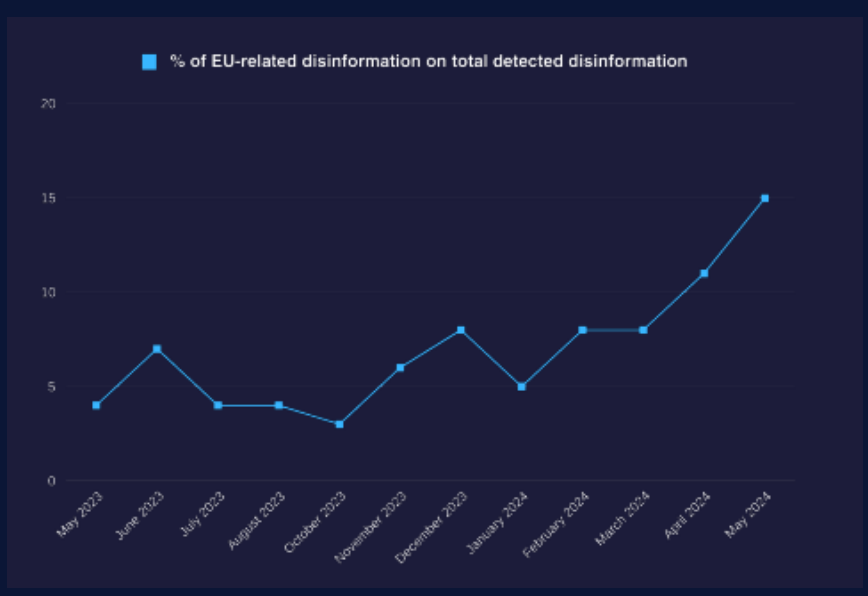
https://online.ucpress.edu/gp/article/2/1/27353/118411/How-Is-Technology-Changing-the-World-and-How

The rapid growth of technology, such as AI and ICT, within today's world has allowed foreign states and organizations to organize clandestine influence operations that are cheaper, more efficient, and extremely dangerous as they pose a detrimental threat to a country's political independence and sovereignty. These operations, ranging from covert funding, AI-generated media, or foreign-controlled apps, can manipulate political discussions and undermine a country's democratic process through a multitude of methods, primarily through disinformation.

Major platforms and social media currently involved such as TikTok, X, and Meta, have dealt with issues of AI spreading deceptive misinformation on their platforms in the past, with some being traced to state actors such as China, in an effort to deceive the public in an election. In 2024, for example, Meta, which owns and operates several large social media platforms such as Facebook, took down around 20 covert influence operations around the world leading up to the 2024 US presidential election. These disruptions were accompanied by AI imitations of the presidential candidates as well as fake accounts that were targeted at citizens to sway public opinion, potentially amplifying harmful narratives and shaping election discourses. In addition to this, operations created by Russia employed AI to imitate news websites such as Fox News in an attempt to weaken Western support for Ukraine, along with fake accounts that were used to manipulate public debate leading to the US election.

To evaluate the exact impacts of foreign technological interference, the EU External Action Service conducted a report on FIMI (Foreign Information Manipulation and Interference Threats), which maps out the digital infrastructure deployed by foreign actors, mainly Russia, to manipulate and undermine democratic processes and societies by spreading disinformation. This report revealed that over 500 FIMI incidents took place across 2024 and were spread across 90 different countries, accompanied by at least 25 different platforms being involved.





In another study done by the European Digital Media Observatory, it was revealed that in the last months before the elections, EU-related disinformation increased from 5% to 15% over the span of a few months, which was the highest among the monitored topics.

Apart from countries in the EU, nations such as Canada have also been targeted numerous times in attempts to affect the results of upcoming elections. For example, foreign states, including India, Russia, and China, have interfered with the country's democratic institutions out of interest for personal gain, as revealed in a report released by the head of the Foreign Interference Commission based on the testimony of more than 100 witnesses.

Currently, it's extremely evident that with the development of modern ICTs and AI technology, numerous threats and security risks arise that could potentially harm a nation's sovereignty and

political independence. Major powers are still debating over what constitutes a “breach” or “interference”, considering the escalation of this issue today, which requires laws and frameworks to be refined and established to avoid these risks. Thus, national agencies and regional bodies such as the EU have been strengthening their defences to ensure no foreign interference takes place; however, international cooperation is instrumental in the development of frameworks that can help ensure this issue is addressed.

UN/International Involvement

Foreign Technological Interference and its Threat to Political Independence has been constantly talked about within the UN General Assembly and all of its committees, with a strong emphasis on technologies such as ICTs (Information and Communication Technologies), and their capabilities in reshaping economies, societies, and international relations. With these immense benefits come risks, as there has steadily been an increase in the malicious use of ICTs, which has posed a massive threat to all States when it comes to harming international sovereignty and political independence. Therefore, numerous NGOs, regional organizations, and the United Nations have been involved in efforts to address this growing challenge.

While SPECPOL does not draft binding resolutions specifically on security threats, the Fourth Committee has still played an important role in forwarding resolutions drafted by other committees of the General Assembly that have addressed Foreign Technological Interference, with an emphasis on the political and communications aspect. An example of SPECPOL's heavy involvement would be Agenda item 53, *Questions relating to information*. This agenda item has proposed draft resolutions addressing the dual challenge of combating misinformation while also ensuring access to information and journalism. Part A of the draft resolution promoted the idea and importance of countering misinformation by strengthening media literacy, while also enhancing international cooperation between developed and developing countries to strengthen communications technology and media infrastructure that is accurate and informative. Part B, *United Nations Global Communications Policies and Activities,* provided suggestions and guidance for the Department of Global Communications to address the increasing spread of misinformation, while at the same time not limiting the important role that ICTs can play in developing countries. (still needs more on the impact of these measures)

Possible Solutions

International Norms and Standards:

The first possible solution is to create general international norms that define what is unacceptable technological interference. Such standards would prohibit cyberattacks against electoral systems, state-sponsored spying into political parties, and intentional spreading of disinformation to destabilize foreign governments. By establishing standards in the United Nations, states would have a framework upon which they could hold one another accountable and reduce uncertainty about what action crosses the line. The main disadvantage of the approach, however, is that enforcement would be insecure because accused states will not admit fault, and powerful actors may oppose binding commitments.

Cybersecurity and Capacity Building:

Another method for SPECPOL is to facilitate capacity-building programs that allow vulnerable states to improve their ability to defend themselves. Developing states lack the technical expertise or economic capacity to maintain capable cybersecurity. Assistance could take the form of training election officials, provision of secure communications hardware, and the funding of infrastructure improvements. It would level the playing field between technologically advanced states and states with lower development. The issue is donor politics and cost, because wealthier states can use aid as leverage to become stronger or pursue their agendas.

Information-Sharing and Early Warning Systems:

Delegates can also consider creating information-exchange channels between governments, NGOs, and IGOs regarding cyberattacks and disinformation campaigns. Having a unified platform to monitor digital threats could allow nations to sense interference sooner and respond in a better manner. Such systems would also have the capacity to validate foreign interference claims. The drawback of the approach is that states will not release sensitive intelligence since they do not wish their vulnerabilities to be revealed, or due to distrust of rival governments.

Diplomatic Accountability:

SPECPOL can recommend the use of political and diplomatic tools that increase transparency and accountability in suspected interference. Instead of sanctions or binding actions, this can be accomplished through General Assembly resolutions condemning interference, calling for states to publish reports on cyber threats, or supporting independent UN reporting documenting incidents

without actually sanctioning states. These measures raise the political cost of intervention by focusing world attention upon perpetrators while remaining within SPECPOL's remit as a recommendatory institution. The drawback of this measure is that it will have a high reliance upon voluntary compliance, and states suspected of interfering will be able to wave off actions in these terms as politically motivated or biased.

Public Awareness and Media Resilience
Finally, long-term solutions may involve strengthening the ability of societies to resist disinformation itself. This may include promoting independent media, demanding fact-checking organizations, and supporting media literacy efforts to provide citizens with an easier ability to identify fallacies. By making citizens more knowledgeable, foreign influence would have less impact on political stability. The disadvantage of this solution is that it takes a very long time to develop, and non-democratic regimes would not be willing to accept such programs as foreign meddling in internal affairs.

Bloc Positions

Western / Democratic Bloc

- Australia – Strongly condemns interference, aligns with the U.S. and allies on cybersecurity norms; heavily targeted by Chinese cyber espionage.
- Canada – Prioritizes election security and countering disinformation; backs international cooperation and capacity-building through the UN.
- France – Seeks strong EU-wide regulation against disinformation (Digital Services Act) while protecting democratic processes.
- Germany – Supports EU regulations and NATO frameworks; wary after revelations of U.S. spying (Snowden leaks).
- Japan – Close U.S. ally; emphasizes protecting democracy from foreign disinformation, especially from China and North Korea.
- Republic of Korea (South Korea) – Faces frequent cyberattacks from DPRK; supports stronger cyber norms and international cooperation.

- United Kingdom – Post-Brexit, maintains strong alignment with U.S./NATO; invested in countering Russian disinformation.

- United States – Pushes for binding international norms against foreign interference; maintains global leadership on cybersecurity but is criticized for surveillance practices.

- Ukraine – Strongly advocates action against Russian disinformation and hybrid warfare; pushes for more robust enforcement.

Authoritarian / Sovereignty Bloc

- Belarus – Aligns with Russia; supports "cyber sovereignty" and rejects Western interference accusations.

- China – Promotes "cyber sovereignty" and strict state control of information; rejects Western accusations while expanding global digital influence.

- Cuba – Opposes Western "information imperialism," emphasizing sovereignty and state-controlled media.

- Democratic People's Republic of Korea (North Korea) – Uses cyber operations as a state tool (espionage, finance hacks); rejects international oversight.

- Iran – Uses cyber influence operations regionally; emphasizes sovereignty and non-interference.

- Russia – Rejects all interference accusations while being a major actor in disinformation; backs sovereignty-first approaches.

- Syria – Supports the Russia/China bloc; emphasizes sovereignty and rejects Western-imposed frameworks.

- Venezuela – Blames foreign interference (esp. U.S.) for instability; aligns with Russia and China on sovereignty.

Non-Aligned / Swing Bloc

- Brazil – As a BRICS member, it balances sovereignty with concerns about election interference; critical of Western firms like Cambridge Analytica.
- Democratic Republic of Congo – Highly vulnerable to disinformation; seeks foreign support to strengthen election security and media resilience.
- India – Promotes "strategic autonomy"; cautious about binding norms but supports global frameworks if they respect sovereignty.
- Indonesia – Advocates non-interference; vulnerable to disinformation; pushes for ASEAN-led approaches.
- Mexico – Wary of U.S. influence; interested in protecting electoral sovereignty but cautious about binding commitments.
- South Africa – As part of BRICS, it aligns with sovereignty-first principles but supports capacity-building for African states.
- Turkey – Plays a middle role; NATO member but also cooperates with Russia; favours sovereignty but opposes interference in domestic politics.
- United Arab Emirates – Prioritizes sovereignty and stability; wary of disinformation campaigns in the Middle East but avoids binding international restrictions.

Discussion Questions

1. To what extent does foreign technological interference violate state sovereignty as outlined in the UN charter?
2. How can the digital divide between developed countries and developing nations be addressed to ensure that all countries have equal capacity to defend themselves from technological interference?
3. What frameworks can be adopted to combat misinformation and disinformation during elections without interfering with freedom of expression and the press?
4. How should the international community define and distinguish between cyber diplomacy and illegal technological manipulation?
5. How do geopolitical rivalries contribute to foreign technological interference?

Additional Sources/Works Cited

Source to help delegates find more info/recommend using

The Center for Strategic & international studies made a full report on creating accountability for global cyber norms. Raising discussions on matters such as sovereign responsibility, political attribution and creating accountability in response to foreign technological interference.
Lewis, James Andrew. *Creating Accountability for Global Cyber Norms*. 5 Aug. 2025, www.csis.org/analysis/creating-accountability-global-cyber-norms.

Stimson's article highlights key events to the UN security council discussion of threats to international security. Addressing the evolving threat landscape and proposing solutions to the matter.
Matamis, Joaquin. "The UN Security Council Discusses Cyber Threats to International Security." *Stimson Center*, May 2024, www.stimson.org/2024/un-security-council-cyber-threats-to-international-security.

The UN security council provided an update on the cyber threats on nations, such as Indonesia, China, and others.
"In Hindsight: The Security Council and Cyber Threats, an Update." *Security Council Report*, www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php.

ASPI raises concern of cyber-enabled foreign interference, like malware and manipulation of voting systems. Providing charts and statistics of violations of foreign interference.
Fergus, Hanson. *Hacking democracies.* ASPI, May 2019, https://www.aspi.org.au/report/hacking-democracies/

The European parliament reports on foreign interference and disinformation in the EU. motions to resolve manipulation of social media, threats to journalists and disinformation of present conflicts.
"REPORT on Foreign Interference in All Democratic Processes in the European Union, Including Disinformation | A9-0187/2023 | European Parliament." © *European Union, 2023 - Source: European Parliament*, www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html.

BRICS battles for digital sovereignty, concerning cyber interference from dominating western countries.
Brics, Think. "BRICS and the Urgent Need for Digital Sovereignty." *Think BRICS*, 8 May 2025, thinkbrics.substack.com/p/the-brics-digital-uprising-why-a.

"Fourth Committee (Special Political and Decolonization)." United Nations General Assembly, www.un.org/en/ga/fourth/ Accessed 29 Aug. 2025.

"Decolonization." United Nations, www.un.org/en/global-issues/decolonization. Accessed 29 Aug. 2025.

Nixon, Ron. "Russia Isn't the Only One Meddling in Elections. We Do It, Too." The New York Times, 17 Feb. 2018, www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html.

Singer, P. W., and Emerson T. Brooking. LikeWar: The Weaponization of Social Media. Houghton Mifflin Harcourt, 2018.

For: Timeline of Key Events & Historical Analysis

Sanger, David E. "The Long History of Russia's Cyber Warfare." The New Yorker, 12 Dec. 2022, www.newyorker.com/news/us-journal/the-long-history-of-russias-cyber-warfare.

"Cyber Operations Tracker." Council on Foreign Relations, www.cfr.org/cyber-operations/. Accessed 29 Aug. 2025.

Smith, David. "Senate Releases Bipartisan Report on Russian Interference in 2016 Election." NPR, 18 Aug. 2020, www.npr.org/2020/08/18/903616315/senate-releases-final-report-on-russias-interference-in-2016-election.

"Moonlight Maze." ScienceDirect, Elsevier, 2023, www.sciencedirect.com/topics/computer-science/moonlight-maze.

For: Current Situation

"3rd EEAS Report on Foreign Information Manipulation and Interference Threats." European External Action Service, 2024, www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en.

Paul, Katie, and James Pearson. "Meta Takes Down Sprawling Chinese-Based Influence Operation Ahead of U.S. Election." Reuters, 5 Sept. 2024, www.reuters.com/technology/meta-takes-down-sprawling-chinese-based-influence-operation-ahead-us-election-2024-09-05/.

"Freedom on the Net 2024: The Global Drive to Control Big Tech." Freedom House, 2024, freedomhouse.org/report/freedom-net.

For: UN/International Involvement

"Questions Relating to Information: Draft Resolution (A/C.4/78/L.12/Rev.1)." United Nations Digital Library, 8 Nov. 2023, digitallibrary.un.org/record/642555.

"Group of Governmental
Experts on Advancing Responsible State Behaviour in Cyberspace." United Nations Office for Disarmament Affairs, disarmament.unoda.org/cyber-state-behaviour/. Accessed 29 Aug. 2025.

For: Possible Solutions

"Tech Accord to Combat Deceptive Use of AI in 2024 Elections." Munich Security Conference, 16 Feb. 2024, securityconference.de/en/news/article/tech-accord-to-combat-deceptive-use-of-ai-in-2024-elections/.

Smith, Brad. "A New Accord to Address AI Deepfakes in Elections." Microsoft On the Issues, 16 Feb. 2024, blogs.microsoft.com/on-the-issues/2024/02/16/ai-deepfakes-elections-munich-tech-accord/.

Carothers, Thomas, and Andrew O'Donohue. "How to Stop Foreign Electoral Interference." Carnegie Endowment for International Peace, 26 July 2019, carnegieendowment.org/2019/07/26/how-to-stop-foreign-electoral-interference-pub-79597.

For: Emerging Threats (AI, Deepfakes)

"AI Deepfakes: The Alarming Rise of Synthetic Media and How to Spot It." Shotkit, shotkit.com/ai-deepfakes-risks/. Accessed 29 Aug. 2025.

"Putin, Kim Jong-Un Deepfake Videos Target U.S. Voters Ahead of Election." The Daily Dot, 4 Nov. 2020, www.dailydot.com/news/putin-kim-jong-un-election-deepfakes/.

Ng, Kelly. "How AI is being used to perpetrate cyber-attacks and disinformation in Asia." BBC News, 21 Mar. 2024, www.bbc.com/news/world-asia-68575651.

For: Regional Case Studies

"Information Manipulation and Foreign Interference: How Congolese Journalists Are Preparing for the Presidential Elections." Fatshimetrie, 20 Oct. 2023, eng.fatshimetrie.org/2023/10/20/information-manipulation-and-foreign-interference-how-congolese-journalists-are-preparing-for-the-presidential-elections/.

Matsakis, Louise. "How WhatsApp Is Fighting Misinformation in India." Wired, 15 May 2019, www.wired.com/story/how-whatsapp-is-fighting-misinformation-in-india/.