The Special Political and Decolonization Committee (SPECPOL)

Topic I : Cyber Espionage and its role in National Elections

Topic II: Addressing the role of Social Media in National Elections

Committee Background

Since 1993, the Special Political and Decolonization Committee (SPECPOL) has been handling the toughest issues in international security and global policy (2). Originally designed to help nations with problems surrounding self-determination and decolonization, an uncharted territory for many new countries, SPECPOL continues to handle the most difficult and unexplored topics at the United Nations (1). SPECPOL takes on many issues before they are moved to the Security Council, as a way of starting discussion, analyzing research and understanding the scope of the problem that may be completely new to delegates before it is moved into more strategic, policy-oriented decisions. SPECPOL's resolutions are not binding, so the goal of this committee is to create the most persuasive and thorough resolutions as to move them forward to other committees with authority. The topics brought forth during this session will be "Cyber Espionage and its Role in National Elections," as well as "Preparing for the Privatization of Space." Only recently has the United Nations, and the world at large, considered these frontiers as part of our global scope. But as the Internet has become the center of world-wide commerce, culture and communication, the issues that have always faced us will continue in the cyber world. With increasing scientific knowledge, space also becomes increasingly accessible, creating endless possibilities for research and business. Every country has a stake in these issues, regardless of thier region, alliances or national power. We challenge you to think deeply and creatively about the problems at hand and understand the challenge behind such modern problems.

Topic 1: Cyber Espionage and its Role in National Elections

Statement of the Problem

As stated in the Universal Declaration of Human Rights, Article 21, "The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures" (3). Nations around the world discuss voter registration, transparency of donation and ballot secrecy as problems in holding a genuine election. But especially after the UK's EU referendum in June 2016, the US presidential election November 2016 and the British election in 2017, cyber attacks seem to be the newest root of unfair elections (5). A foreign government, domestic extremist group, or single individual now has immense power to impact a national election, changing the way we all think about the democratic process. Free elections are a basic human right that must be protected by this committee and the UN at large, and cyber espionage can undermine this fundamental liberty. The problem is clear: how do countries protect themselves from such attacks, as well as engage in positive relations with their own citizens, to fulfil the people's right to a fair and just election. The solutions are endless, and much more complicated.

History of the Problem

Spying, sabotage, and subversion have always been part of international warfare, and after the rise of the internet in the 1990s, cyber espionage was soon to come. It's difficult to pinpoint the first cases of cyber espionage because, due to the nature of the internet, lots of actions are untraceable and were not understood in the early days of the web. The first documented case of cyber espionage, however, was in 1986, before the internet itself (5). A hacker had been systematically targeting computers at military bases around the US, looking for military secrets. The hacker was caught but it was the first time the US government even considered the possibilities for this kind of crime on computers. In 1999, the first major case of cyber espionage appeared in the US. An FBI investigation found that a group had stolen documents from the US Navy, Air Force, Department of Energy and NASA (9). Between 2005 and 2010, global cases of espionage started appearing, mainly with individuals or groups attacking government entities or businesses. Google disclosed that it, as well as other large companies, had been targeted by a group called Aurora, which had the capability of carrying out hundreds of attacks on these businesses. Stuxnet also appeared in 2010, a piece of malware that gained worldwide attention by attempting to hijack Programmable Logic Controllers, the component that run and monitor industrial systems (9). The PLC it was after was being used by the Iranian uranium enrichment program, which was the center of enormous diplomatic discussion. This was the first time that the global community really considered the possibility that this technology could be used between two states, as a replacement for traditional warfare. Another destructive bug was used in multiple attacks against the Saudi Arabian energy sector. Although the uses of such bugs has changed, the idea that cyber attacks and government relations and politics are completely interconnected, has not. Multiple high profile leaks occurred after the boom of malware, including the leak of sensitive NSA information by whistleblower Edward Snowden and the publishing of Vault 7 by Wikileaks in 2017 (8). These leaks detailed the activities and capabilities of the United States CIA to perform their own electronic surveillance and cyber warfare. Governments clearly use their own forms of surveillance both for security and information, to different degrees, but it raises the question: when are these tools used maliciously and when are they not? We must consider when such information is shared or how it can be used to distort the views of the public, possibly threatening elections worldwide.

Current Situation

The US indictment of 13 Russians and three Russian companies for spying via social media caught the world's attention at the beginning of 2018. US Special Counsel Robert Mueller carried out the investigation after much discussion about tampering with the 2016 US election. The general verdict was that Russian hackers broke into the computer network serving the Democratic National Convention (10). In July 2016, WikiLeaks published emails from the accounts of senior party staffers and had access to all memos and research on the server. This impacted the rhetoric in US debates and the validity of the candidates. After investigations, it was found that Russia had already been carrying out such attacks in Syria and the Ukraine, as well as possibly other Eastern European countries, attempting to skew the elections in their favor (8). After the 2016 US election, global conversation stirred about how to stop such attacks and the reasoning behind it. Governments must balance between their own uses for intelligence and surveillance and the inappropriate foreign interference that can change the minds of voters and the outcome of elections.

In Cambodia, Chinese cyber spies have targeted government institutions and opposition party members to gather information ahead of elections in summer 2018. The hacks are thought to have come from the Chinese cyber espionage group, TEMP. Periscope, who have also been linked to tampering with American engineering companies' interests in the South China Sea. It is unknown the exact tactics China will use to keep Prime Minister Hun Sen in power, but we do know that during his 30 years in office, China has become Cambodia's biggest donor, trading partner, and investor. Cambodia has also become a key supporter of China's interests, meaning that the draw to secure the Cambodian election is evident.

There is agreement that such crimes should be prevented and prosecuted but it is difficult to decide what jurisdiction and laws apply online. UN Secretary General Guterres commented saying, "There is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it." He continues saying that he believes that the next war will "begin with a massive cyber attack to destroy military capacity". These powers are not to be underestimated but he reaffirmed that the UN can be a neutral space to discuss such matters. NATO allies have been working on an agreement to guide their militaries on how to use and protect from cyber attacks which they intend to publish next year. SPECPOL delegates who are also involved in NATO can continue thinking about the justifications for a cyber attack and protection measures that not only apply to those countries, but to all UN member states.

Directive/Possible Solutions

- If a concern is that foreign currency is being sent to campaigns online, there could be a decision to bring more transparency to political ads on the internet as those on TV and radio, and explicitly ban the purchase of political ads by foreign nations for elections.
- Require licensing for all foreign sourced media accounts that want to advertise or disseminate information above a certain monetary level. This was a concern in the US election, that Russians were buying internet ads to influence voters.
- Work with the private sector, including social media companies, to ensure transparency surrounding election rhetoric. This would also come with additional support and protection for companies against cyber espionage groups.

- Universal condemnation for groups/countries that have tampered with foreign elections as well as sharing with the global communities the gaps that lead to such tampering and possible solutions to such issues.
- Start counterintelligence to detect foreign intelligence operations that may be interfering with elections. This could then be stopped directly before the election takes place.
- Tightening of national voting procedures to guarantee no external forces are acting or influencing voters. This could include protecting the registration software or electronic ballots.
- Start research efforts to expose the use of trolls, bots or ads in past tampered elections to have a greater idea of the current state of cyber espionage

Possible Bloc Positions

- Think about nations that would like to see your country's political leadership stay the same or change. Consider how to keep allies while maintaining integrity in elections.
- The US and Russia will be able to discuss 2016 election tampering, and lessons to be learned from such events.
- The Ukraine and Syria can also consider how their relationship to Russia has been impacted by the 2016 election.
- Saudi Arabia and Iran can consider how western views of, and actions in, the Middle East impact your elections.
- China and Cambodia can discuss the upcoming Cambodian election and how China's stakes in the current leader may be impacting surveillance.
- The UK can discuss Brexit and the 2017 election, and how cyber espionage has impacted the British political system.

Key Terms

Cyber espionage

A form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity.

Signals Intelligence

The monitoring, interception, and interpretation of others' information and communication

Works Cited

(n.d.). Retrieved from http://www.inss.org.il/publication/the-superpower-cyber-war-and-the-us-elections/

(n.d.). Retrieved from https://www.bloomberg.com/news/articles/2018-07-11/chinese-cyber-spy-hackers-target-cambodia-as-elections-loom

(n.d.). Retrieved from http://www.inss.org.il/publication/the-superpower-cyber-war-and-the-us-elections/

Gray, A., Dallison, P., & Young, Z. (2018, May 22). US elections are under threat from cyberattacks - and so are yours. Retrieved from https://www.politico.eu/article/all-elections-under-threat-cyberattacks/

Khalip, A. (2018, February 19). U.N. chief urges global rules for cyber warfare. Retrieved from https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cy ber-warfare-idUSKCN1G31Q4

O'Brien, D. (2017, July 27). A short history of cyber espionage – Threat Intel – Medium. Retrieved from https://medium.com/threat-intel/cyber-espionage-spying-409416c794ec

Stewart, E. (2018, February 19). Russian election interference is far from over. I asked 9 experts how to stop it. Retrieved from https://www.vox.com/policy-and-politics/2018/2/19/17023240/election-2018-russia-inter ference-stop-prevent

The United Nations and Decolonization. (n.d.). Retrieved from http://www.un.org/en/decolonization/fourthcomm.shtml

United Nations, main body, main organs, General Assembly. (n.d.). Retrieved from https://www.un.org/en/ga/fourth/index.shtml

What is Cyber Espionage? | Cyber Espionage Definition. (n.d.). Retrieved from https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/

Thank you

UNA-Houston and Global Classrooms would like to thank the University of Texas at Austin and give full writing credits of this background guide to Finlay Scranton a student at UT-Austin. The mission of Global Classrooms is to introduce students from lower socioeconomic backgrounds to a realm of international relations and diplomacy. We target Title 1 schools in the Houston area and give them an affordable opportunity to attend a Model UN conference.

Original Background Guide Link

https://static1.squarespace.com/static/54d7b4b0e4b0a551f3b29a36/t/5b8ffd614d7a9cdf89ec6270/1536163169442/SPECPOL+1+%282%29+-+Finlay+Scanlon.pdf