CalsMUN 2020

Historical Influences

Research Report

Forum: General Assembly 1

Issue: Cyber interference on democratic processes

Chairs: Michou van de Rijke and Ramon Groenwoud

Personal Introduction

Michou van de Rijke

Hello, my name is Michou van de Rijke and I am currently attending Cals College Nieuwegein. I am 17 and in my sixth year of pre-university education (VWO). I enjoy reading, chatting with my friends (or talking in general) as well as binge watching hours of content of my favourite creators on YouTube (such as but not limited to Jolly, Drew Durnil & ClickForTaz). Furthermore, I am a figure skater (though not a very good one) and normally spend my Saturday morning in the ice rink.

My first MUN experience was at CalsMUN in the GA1, I am therefore very happy to be assist new MUN'ers as well as experienced delegates in the upcoming weekend in said committee. This conference will be my ninth, and I hope to chair fruitful debates as well as fun ones.

Ramon Groenewoud

Whatup delegates,

My name is Ramon Groenewoud and I'm 16 years old. I'm now in my fifth year of vwo on the Farel college in Amersfoort, the home of FAMUN. I love doing sports such as but certainly not limited to tennis, soccer, snowboarding and wakeboarding. I started participating in MUN's a little over a year ago and couldn't stop anymore. This conference will be my seventh conference in total, but my first Calsmun ever. My lifelong tip for people that want to learn English is: Watch YouTube and Netflix. Of course, I listened to my own advice, therefore watching Netflix and Youtube is another thing I do in my spare time.

Introduction

The essential values of a democratic country are liberty, equality, participation, and civil rights. A crucial characteristic for a democratic country is the holding of general, free elections that take place at intervals as prescribed by law. Elections are the ultimate expression of the democratic process and constitute a key component in the building of the public's confidence in a country and the faith of its citizens in its institutions.

In recent years, we have seen attempts of external interference and subversion of the election processes in many democratic countries throughout the world through cyberattacks (examples include the election in 2016 of the United States). Cyber threats to the election process in democratic countries may be categorized as threats that aim to disrupt the process through technological tools designed to corrupt information systems and the polling and voting systems, and as material threats to democratic institutions by sullying their good name and by undermining the public's faith in them. While the first category of threats is well known, and some countries are well prepared to contend with them, the second—which is more abstract—is a new type of threat that requires appropriate consideration as well as analysis.

Definition of Key Terms

Democratic country

A democratic country is a country that's ruled by its people or agents elected by them in a free electoral system. In other words, a democratic country is one where its people have a high degree of civil as well as political freedom. Partial democratic countries have a low degree of either or of both.

Cyber warfare

Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks.

Cyber espionage

The use of computer networks to gain illicit access to confidential information, typically that held by a government or other organization.

Cyber sabotage

The deliberate and malicious acts that result in the disruption of the normal processes and functions or the destruction or damage of equipment or information.

Hacktivism

The act of misusing a computer system or network for a socially or politically motivated reason.

General Overview

Firstly, more technologically developed states are inherently more vulnerable in cyberwarfare. Large developed countries have the capability to have more electronic infrastructure to defend; the larger your network, the more vulnerabilities you present to your attacker. Stronger actors have more to lose than weaker actors do in cyberwarfare.

Before the Internet, interference in democratic processes involved costly training and movement of spies across borders, establishment of foreign bank accounts, and transfers of cash. Now however, similar effects can be accomplished remotely and at much lower cost. It is much easier to send electrons across borders than human agents. Ransoming a failed spy can be costly, but if no one clicks on a phishing e mail, it is simple, deniable, and virtually free to send another. In 1983, when the KGB seeded the rumor that AIDS was the product of U.S. government experiments with biological weapons, the rumor started with an anonymous letter to a small New Delhi newspaper and then was propagated globally but slowly over several years by widespread reproduction and constant repetition in conventional media. It took four years to reach full fruition. In 2016, an updated version of the same technique was used to create “Pizzagate,” the rumor that Hillary Clinton’s campaign manager ran a child sex ring in a Washington restaurant. It spread instantly on the Internet. What’s new is not the basic model; it is the speed with which such disinformation and ‘fake news’ can spread and the low cost of spreading it.

Democracies, too, have used cyberattacks against non-democratic states. Perhaps the best known example is the use of ‘StuxNet’, the successful attack, most likely by the United States and Israel, involving a malicious computer worm that sabotaged an element of Iran’s nuclear program. Other countries with similar capabilities could be stealthily using them against their rivals. As a member of former President Barack Obama’s council of advisers on science and technology said: “The internet is now fully weaponized.”

Yet, so far, the main *political* victims of cyberattackers have been leaders and public figures in democratic countries—especially the United States. And the United States is not the only democracy vulnerable to political cyberattacks. One of the conclusions of the intelligence community's report on the 2016 election hacks points to a much broader implication: "We assess Moscow will apply lessons learned from its Putin-ordered campaign aimed at the U.S. presidential election to future influence efforts worldwide, including against U.S. allies and their election processes."

Another issue is the question if it is possible to determine, if, and at what point acts of interference equal a violation of sovereignty—or beyond that, an act of war?

And finally, the hallmark of democracy is exposition, not to make your position unassailable but to invite debate and conflict and discussion. To be able to spark debate and discuss what the new normal is, we need to roll up our sleeves and get dirty.

Major Parties Involved

Organisations

European Union

The EU said in June that it would conduct war-games to prepare for any cyber-attacks, signaling the bloc's determination to increase co-operation against any supposed Russian and Chinese meddling.

Countries

Russian Federation

In countries like France, the Netherlands and Ukraine, Russian Federation has allegedly used its influence on operations to affect political campaigns, candidates, and discourse to attack perceived opponents of Putin's Russia and support those more sympathetic to Russian interests. The focus of Russia's cyber operations also tends to be strategic and long term in nature, rather than operational or tactical.

Democratic People's Republic of Korea

Experts have begun to question whether North Korea's cyberwarfare capabilities pose as great a threat as its nuclear arsenal. Since the early 2010s, hacking attacks from the North have increased in frequency – from one attack in 2015 to four in 2017, and four last year as well.

United States of America

As a result of the nature of cyberwarfare, the United States' economic and military advantages are diminished. In this case, the disadvantaging effect of cyberwarfare does not apply only to the United States, but all conventionally powerful states.

The United States is the society most reliant on its information systems and infrastructures. According to Pentagon officials, massive networking are making the US the world's most vulnerable target for information warfare. The US has orders of magnitude more to lose from information warfare than its competitors. Not only does the United States more vulnerable to attacks, but it also risks more when attacking—because the American cyber infrastructure is so large. If the United States were to engage in sustained cyberwarfare, it simply has more to lose than any other actor in the system.

Republic of China

Though many of the allegations focus on the tension between China and the United States on cyber espionage, these actions are unlikely to cause armed conflict since almost all capable actors are conducting cyber espionage.

Suspicions of intentions and capabilities of cyber warfare, however, could drag the US and China into arms races, due to the role cyber tools can play in military operations.

Timeline of Key Events

Date	Description of Event
2007	Estonian government networks were raided by a denial of service attack by unknown foreign intruders. The sophistication of this cyber-attack was one of the earliest of its kind.
2009	The US Cyber Command is established on the order of the Secretary of Defense.
2013	The Tallinn Manual, an academic, non-binding study on how international law applies to cyber conflicts and cyber warfare is published
2016	Russian alleged interference in the US presidential elections

Previous Attempts to Resolve the Issue

In 2011, the Shanghai Cooperation Organization (SCO) proposed the International Code of Conduct for Information Security to the United Nations General Assembly (UNGA). This code aimed to progress the international efforts to develop standards for behavior in cyber space. The code did not pass the vote in the UNGA in 2011 due to the excessive internet censorship contained in its principles. However, the SCO amended the code to take into full consideration the comments of all parties and proposed it to the UNGA for a second time, in 2015. The code did not receive a majority in the second vote, which took place in the UNGA's September 2015 session. It is speculated that this is due to the concerns that the code raises with regards to human rights. The code emphasizes state sovereignty as a priority above all else and reflects that the SCO seeks the revising of international human rights law.

Possible Solutions

Teamwork. Fighting hackers from just about every corner of the globe is an enormous task but doing it by yourself makes it even harder. That's why a growing number of state governments are creating multiagency groups to tackle cybersecurity.

Impartial centers. Perhaps internationally supported, impartial centers could be created with the task of identifying and countering inaccurate (or misrepresented) information that is spread on the internet, and information that could pose as a threat to modern-day democracy. These could further limit the threat of cyber interference in participating states. They could also play a role in developing legislation regarding the issue that is focused on the quick development of technological advancements. Such centers would enable member states to share their knowledge of this issue and any developments associated with it.

Employee training. When it comes to security, government CIOs are haunted by the old cliché, "You are only as strong as the weakest link." To counter this problem in government, states and localities could developed what is known as security awareness training. The idea is to make government employees more conscious of security overall and to reduce the kind of mistakes that can launch an intrusion, trigger an attack or inadvertently allow certain types of fraud.

Understanding. One could think about reaching an internationally-accepted understanding of cyber security which could enable member states to move forward with a more unified interpretations of legislation that discusses cyber issues.

Further Reading

https://www.hoover.org/research/protecting-democracy-era-cyber-information-war

https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html

https://css.ethz.ch/en/services/digital-library/articles/article.html/6690e2b2-bd9e-40ef-aabb-185d8a449116/pdf