# Geopolitics and the Digital Domain: How Cyberspace is Impacting International Security

Georgia Wood
*SIT Study Abroad*

# Geopolitics and the Digital Domain: How Cyberspace is Impacting International Security

By Georgia Wood

Spring 2020

School of International Training (SIT)

Geneva: International Studies and Multilateral Diplomacy

Dr. Gyula Csurgai, Ph.D.

University of Michigan, Ann Arbor

International Studies: International Security, Norms, and Cooperation

## Abstract

The digital domain is the emerging environment for which the internet and data connectivity exists. This new domain is challenging the traditional place for geopolitics to exist, and creating new challenges to international relations. The use of cyberweapons through direct cyberattacks, such as the possibility of an attack on the U.S. power grid, or misinformation campaigns, such as the one launched by Russia against the 2016 U.S. Presidential election, can expand the international threat landscape. While these new threats increase, states are widely not prepared to address the new challenges in the digital domain. This paper will use three primary sources and a variety of secondary sources to analyze the aspects of cyberwarfare, how to effectively secure nations against threats from the digital domain, and how developing versus developed countries react differently to advances in technology.

## Acknowledgements

I would like to thank Dr. Csurgai for being an instrumental part in the creation and development of this paper. Additionally, thank you to Aline and Christine for your help in making my time in Switzerland so impactful.

Thank you to the wonderful 26 other students in the SIT International Studies and Multilateral Diplomacy program. Even though our time in Switzerland was cut short, thank you for the constant support and friendship throughout our two months.

**Table of Contents**

## Introduction

### Why it's Important to Study Cyberspace in the context of geopolitics

While geopolitics has been advancing and tackling new challenges for centuries, the development of a cyber domain is creating a new space for geopolitics to exist. The cyber domain in the context of geopolitics refers to the use of the internet or digital operations in achieving one's political agenda. While many security and diplomatic experts address the need for digital strategies in combating disinformation and cyberweapon campaigns, there is little discussion on how this domain will shift the area of geopolitics. It is necessary to look at the totality of what geopolitics encompasses, from economic means to security, in order to better understand how the cyber domain will expand international relationships.

While during our time in Switzerland we studied a variety of geopolitical issues such as migration, terrorism, economic security, etc, there was only one lecture on the digital domain and it focused on the diplomatic side of international studies. I want to focus my research project on how geopolitics is shifting due to the increase in cyberweapons and how this will impact spaces in geopolitics. I expect my paper to highlight how much of the world is unprepared to address cyberweapons and their impact on geopolitics.

### The Focus of the Study

While it is important to cover all relevant material relating to the geopolitical sphere of the digital domain, I will be touching on the following aspects to keep my study brief. First, there will be a discussion of the definition of geopolitics and how cyber weapons are challenging this definition. Next, it is necessary to define what are the most threatening cyber-attacks to international security with a case study on the U.S. power grid. Following that there will be a section on who are the actors participating in the digital domain. After, there will be an analysis of the cybersecurity aspects of this new space and how the European Union is creating incohesive cybersecurity policies. Next, a discussion on the economics of the digital domain will be presented to reveal how developing and developed countries are impacted differently by this space. Finally, the paper will end with insight on what the future for the digital domain will look like, specifically focusing on recommendations for securing the cyber sphere. Overall, this paper will answer how the space for geopolitics is being impacted by the digital domain and it will provide recommendations for how to handle this new space in international relations.

## Literature Review

The literature surrounding the digital domain and geopolitics often is limited in its scope of focus. While there are a variety of publications available, a large portion does not specifically mention geopolitics. Additionally, most of the literature available focuses strictly on one aspect of the digital domain, such as economics, security, or the type of warfare used. There is a little amount of literature that looks at the digital domain from a holistic stance, considering the wide array of aspects impacting cyber space.

However, a large number of publications on the digital domain and geopolitics come from the Center for Strategic and International Studies (CSIS) Technology Policy Program, International Security Program, and Strategic Foresight Group. The most important recent CSIS pieces of literature that relate to my ISP topic include *Cyber Solarium and the Sunset of Cybersecurity*, *Economic Impact of Cybercrime*, *Russia's Attacks On Democratic Justice Systems*, and *Has Europe Lost Both the Battle and War over Its Digital Future?* These reports use a data-driven approach to understanding the issues facing the digital domain today.

In addition to CSIS, the Institute for National Security Studies (INSS), an Israeli-based think tank has a "Cyber, Intelligence, and Security" program that highlights new developments in cyberspace. The INSS Cyber, Intelligence, and Security releases a report every month about the most relevant developments impacting cyberwarfare, with the most recent addition being *The Secret War of Cyber Influence Operations and How to Identify Them*. These reports look past the case by case basis of cyber conflicts and look to compare traditional means of military tactics to cyberwarfare.

Relevant literature surrounding this topic also includes reports released by governments on the issue of cybersecurity. Specifically, the White House released a report entitled, *The Cost of Malicious Cyber Activity to the U.S. Economy.* This report highlights the risks of a cyber-attack to the United States, while also describing the United States' policies surrounding cybersecurity.

The theoretical approach in this study will compare historical geopolitical spaces to modern cyberwarfare. In addition to defining geopolitics and how historically it has been used, the project will address the new issues that arise with the advancement of technology. In general, the study aims to address how technology and cyberweapons are shifting the space of geopolitics. While wars have been fought in a variety of spaces—air, land, and sea—the cyber domain creates another space for geopolitics with new problems to address.

**Research Methodology**

This research project includes both primary and secondary sources to help develop an analysis of how the digital domain is shifting geopolitics. The primary sources utilized include three different interviews with experts based in Europe. One of these interviews was conducted in person in Brussels, Belgium and the other two were accomplish through phone calls due to the coronavirus pandemic. These experts come from a variety of backgrounds including experience with artificial intelligence, European Union cybersecurity policies, digital diplomacy, cyberwarfare, misinformation campaigns, and general knowledge of how geopolitics are being impacted by cyber tools. In addition to the primary sources, there is also the use of secondary sources to complement the primary sources used. To draw from the best and more accurate sources, the University of Michigan library database that allows students access to thousands of scholarly articles online was referenced. Since the paper includes three expert interviews, there was also a consultation with the CYBERSEC Forum that happened in March of 2020. While this conference was supposed to be in person, a digital version was produced and published to YouTube. The paper references this conference in a variety of sections to gain a better perspective of European approaches to cybersecurity strategies.

The study primarily used qualitative analysis methods to analyze the primary and secondary sources presented in the development of the research question. The largest aspects of qualitative analysis that were used include interviews and content analysis to better understand relevant narratives around the topic. While the majority of the paper was done through qualitative analysis, there was a significant amount of secondary quantitative analysis tools. For example, Gallup polls and statistical modeling was presenting as a way to support arguments, but the analysis was done by a secondary source.

In terms of the ethical considerations of this study, there were a variety of considerations necessary to align with the guidelines of the School for International Training (SIT). First, throughout the expert interviews, an acknowledgment of the rights of the subjects was necessary to address and a clear path for open communication was established. Additionally, in presenting and processing relevant data to the study, acknowledging and accurate presentation of sources was necessary. Finally, before beginning the study, an application to the SIT ethical review board was completed regarding the use of human subjects.

**Definitions and the Analytical/Theoretical Framework**

There are a variety of terms that can be used to describe how the internet and digital connectedness of the globe is impacting geopolitics. While many of the terms refer to similar concepts or items, there are some differences that should be noted prior to reading the analysis section of this paper. The digital domain refers to the internet, connection of cyber tools, and any software that exists in the cloud. Often, when using the phrase digital domain, it refers to the new sphere created for geopolitics to exist with the advancement of technology. Cybersecurity is the aspect of protecting the digital domain from adversaries. Cyber weapons are any cyber tools that have been created to cause disruption or harm to an actor. Cyber space is similar to the digital domain in referring to the sphere created by technological development. Geoeconomics is the economic trends of countries and how they relate to other nations. Finally, cyber warfare is how states and non-state actors utilize cyber tools to cause destruction.

**Defining Geopolitics and its Historical Space**

Historically, geopolitics has been defined as “the interactions between political processes and geographic spaces, not as a separate social science but as an interdisciplinary method of analysis” (Csurgai 2019). The most important aspect of this definition is the aspect of “geographic spaces”, representing the traditional means of geopolitics occurring in physical spaces such as land, air, and sea. The tangible aspects of geopolitics such as natural resources, geographical configuration, and the geography of populations have historically contributed to the relationship between geopolitics and space. One of the most important developments of the early 21st century was the rapid commercialization of air space. From 1970 to 2001, airline passengers increased by 1.345 billion passengers carried every year (Air transport, passengers carried 2001). The commercialization of the air domain for geopolitics advanced swiftly, allowing the space to be a target for actors to achieve political goals. This was mostly seen in the events of 9/11, where a terrorist organization utilized this new space in geopolitics. In comparison, a similar but larger development in the space of geopolitics today is occurring with the creation of a cyber domain.

The cyber domain is adding a new space for geopolitics to exist, creating a relationship between political processes and the digital sphere. Over 4.39 billion people are currently online, which demonstrates a rapid increase in users from the creation of the world wide web in 1990. However, it is not just users on the internet, digital tools are now a part of every part of modern society. This new space creates a variety of new developments for geopolitics, ranging from security implications to economic incentives. In general, the cyber domain does not solve or delay current geopolitical conflicts, but rather “the Internet seems to multiply and complicate them” (Douzet 2014). Due to the creation of this new domain in which geopolitics exists, it is necessary to examine the impact cyber will have on the future of international relations.

While the cyber domain is impacting geopolitics in a variety of ways, it is important to understand it is the means of international relations, not the underlying interests that are being impacted. James Lewis of the Center for Strategic and International Studies (CSIS) highlights this impact in noting that “despite the digital revolution, the strategic interests and objectives of states remain unchanged for the time being” (Douzet 2014). With the advancement of the internet and cyber tools, the means of geopolitics is shifting, but the motivating factors of nation-states remain the same. The new means of geopolitics that the cyber domain has created have led to a significant amount of new threats to international security, including cyberweapons, misinformation campaigns, and economic warfare. These threats will be addressed in future sections, specifically how actors and countries are responding to the shift of geopolitics in cyberspace.

## Actors and Aspects of Cyberwarfare

### Non-State Actors

There is an increased amount of actors now participating in the digital domain and while the realities of cyberwar are seen more as a future than an immediate threat, “one of the most remarkable elements of past cyber events is the substantial involvement of non-state actors” (Bussolati 2015). For these groups, the digital domain became a place to spread their political ideologies and utilize “digital weapons—cheap, powerful, and easy to use, to obtain, or to manufacture” (Bussolati 2015). A variety of non-state actors are able to use the digital domain to achieve their objectives, including individual hackers, criminal organizations, cyber mercenaries, or hacktivists (Bussolati 2015). Some of the largest successful hacks, such as the 2007 Estonian denial of service attack, have been committed by non-state hacking groups (Bussolati 2015). These groups have increasingly turned to digital tools to achieve their objectives due to the anonymity of cyberweapons and ease of access to these resources. A recent study estimates that a low-end cyberattack that costs just $34/month could return $25,000 a month to the hacker (Friedman 2016). In addition, these low-cost cyberattacks can advance the political agenda of a non-state actor in a variety of ways. While there are many ways non-state actors are utilizing the digital domain, some barriers exist to full access to cyber tools by these groups.

## State Actors

In comparison to non-state actors, state actors are taking a different approach to utilize cyber tools in the digital domain. There are three areas that states are focusing on to tackle threats in the digital domain—public/private partnerships, collaborations across states, and understanding the diversity of threats—however, there are many areas for states to improve in these categories.

First, since the digital domain relies so heavily on private companies creating new advancements, states will be at the forefront of technological development if there is a focus on public-private partnerships (Duberry 2020). If states are able to collaborate with private companies to lead the advancements occurring in the digital domain, they will always have the advantage over non-state actors of utilizing these resources first and developing security measures to protect against these advancements. However, there is little cooperation existing between the public and private sectors for a variety of reasons (Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms 2018). Primarily, the lack of an information-sharing platform between the public and private sectors creates disparities in technological development between states and companies (The Cost of Malicious Cyber Activity to the U.S. Economy). Additionally, states struggled with sharing information about their cyber strategies to the public, out of fear adversaries will use it to their advantage. It was not until the Trump administration took office in 2017 that the United States publicly displayed the pillars of their cybersecurity strategy (The Cost of Malicious Cyber Activity to the U.S. Economy). This lack of transparency made it more difficult for private companies to work with the public sector in advancing the cybersecurity capabilities of the federal government.

Next, as non-state actors act alone in separate groups with little collaboration, states are creating partnerships to ensure protection against cyberweapons. Global cyberattacks, such as the WannaCry ransomware attack of 2017 on civilians that locked people out of their devices until a sum is paid to the hacker, created the understanding that international cooperation is necessary to fight these non-state actors (Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms 2018). Not only do global attacks allow countries to understand the security threat cyberattacks create to their citizens, but the WannaCry attack cost over $1 billion dollars and demonstrated the economic impact non-state actors can have using cyberweapons (Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms 2018). Legislation across the European Union has been enacted to create uniformity in cybersecurity policies, but there are still significant gaps in these regulations that expose states to cyberattacks (Fantin 2020). There will be a significant discussion on the lack of uniformity in the EU cybersecurity policy later in the paper.

Finally, there is some concern about the diverse amount of security threats that are created in the cyber domain and the ability of states to be prepared to face these threats. While other spaces for geopolitics to exist have widely remained constant in their threats, the digital domain is developing more rapidly than ever seen before (Duberry 2020). Instead of being natural-born like air, land, and sea, the digital domain is man-made, allowing people to have the power to change and advance it (Duberry 2020). One of the more recent threats that the digital domain has produced is the advancement of misinformation campaigns being spread on social media. Cognitive warfare such as these misinformation campaigns is having a large impact on geopolitics and international relations as a whole.

## How the U.S. Power Grid Represents Vulnerabilities in the Digital Domain

In addition to cyberspace transforming the geopolitical landscape, the cyber weapons used now create new threats to international security. Not only is the cyber domain shifting how we understand international relations and expanding our understanding of geopolitical spaces, but the development of digital weapons creates more advanced threats to our civilizations. One of the largest concerns is the “protection of vital infrastructures, which if disrupted or sabotaged could endanger civilian populations” (Douzet 2014). In a highly digitized society where basic security requirements and natural resources rely on the cyber domain, there is an increased geopolitical threat to citizens (Dincic 2020). The largest example of a vulnerable aspect of infrastructure includes the digitalization of the power grid across the globe, more specifically the United States’ power grid is especially vulnerable to an attack by an adversary.

Specific vulnerabilities in the U.S. power grid system demonstrate how hackers could gain access and control over the North American power grid. The power grid is initially designed to protect itself from natural disasters or cyber-attacks because it is broken up into 4 sections across North America. However, if adversaries can take offline 9 substations out of the 55,000 in the United States, the U.S. could suffer coast to coast blackouts lasting 18 months or more (U.S. Risks National Blackout From Small-Scale Attack 2014). In March 2019, a cyber-attack on critical power centers demonstrated the specifics of how an attack can harm U.S. infrastructure.

The cyber-attack in March 2019 attacked parts of the power grid in California, Wyoming, and Utah using a vulnerability in the network’s firewall (Report reveals play-by-play of first U.S. grid cyberattack 2019). The utility’s firewall censored data flow from the grid’s generator sites to the utility’s control center. The hacker utilized this vulnerability to reboot the firewall over and over, eventually breaking the software and making operators lose contact with the generator sites and the control center. These glitches lasted for around 10 hours, but power was never lost to any of the power grid sections (Report reveals play-by-play of first U.S. grid cyberattack 2019). There is evidence that the attacker was most likely using an automated bot to scan the internet for vulnerable devices and did not know it had infiltrated the utility's network.

Future attacks could happen similarly to the cyber-attack that occurred in March 2019, but there are also other ways an adversary could infiltrate the North American Power Grid (The Cost of Malicious Cyber Activity to the U.S. Economy 2018). According to the White House, adversaries could target laptops of key personnel with access to multiple power plants, physically enter locations that monitor the power grid network, or hack a remotely accessed control system. Additionally, the White House fears phishing attacks against the power grid's corporate network to infiltrate the system and then use a pivoting attack to ultimately access the control system (The Cost of Malicious Cyber Activity to the U.S. Economy 2018). All these methods expose vulnerabilities to the North American Power Grid that could allow adversaries to cripple the U.S. and have major impacts on Americans.

An attack on the North American Power Grid could have large effects on the U.S. economy, health and human rights of U.S. citizens, and threaten national security. First, the economic impacts can be seen through the largest power outage in U.S. history in 2003 that impacted the Midwest, Northeast, and parts of Canada. This outage was because of a human programming error with indirect and direct damages costing a total of $6 billion (Emerging Risk Series, Business Blackout 2015). Recent estimates project that a cyber-attack on critical U.S. infrastructure could cause economic damages up to $1 trillion (Emerging Risk Series, Business Blackout 2015). In addition to economic implications, a cyber-attack could cause health and safety concerns for U.S. citizens. A power outage would impact heating and cooling for homes and food supplies, limit the supply of clean water without power for the treatment pumps, and create a fuel shortage in hospital generators (The Cost of Malicious Cyber Activity to the U.S. Economy 2018). All of these implications could cause severe illness and death in the U.S. Finally, 85% of the Department of Defense's (DoD) energy comes from commercial services and a power outage would greatly impact the defense of the United States (The Cost of Malicious Cyber Activity to the U.S. Economy 2018). The DoD would be unable to perform routine protections against adversaries to secure the U.S. The impact of a cyber-attack to the North American Power Grid would have severe financial, humanitarian, and national security implications on the United States.

**Misinformation Attacks**

The rapid expansion of social media has led to a new geopolitical threat to states across the globe. As of January 2020, there were over 3.8 billion social media users across the world (Digital in 2020). This new platform has connected the world in incredible ways, from fueling the Arab Spring to giving people in underdeveloped countries access to the internet. However, with the rise of social media, there is also a rise in geopolitical threats that face societies. Across the globe "many countries use cyberspace, and specifically social media, to manage cyber influence operations as part of holistic information warfare" (Tayouri 2020). These misinformation campaigns serve a variety of purposes and they are not the first time influence operations have been utilized in warfare, "a close term to cyber influence in the military context is influencing maneuver, which is the process of using operations to get inside an enemy's decision cycle or even forcing that decision cycle to direct or indirect actions" (Tayouri 2020).

While these types of operations have appeared in military tactics before, misinformation campaigns in the digital domain create a vast array of new threats to geopolitics.

The most prominent and impactful use of misinformation spread on social media came from Russian forces beginning in 2014 all the way up to the 2016 U.S. Presidential election. Specifically, the hackers deployed “social media trolls and bots to spread online content that undermines faith in democracies and their institutions” (Spalding 2019). This campaign had a large impact on civil society with approximately 126 million people being reached through Russian posts on Facebook during the 2016 presidential election (Spalding 2019). These posts were not simply in support of one candidate over another for President of the United States, Russia was pursuing “an attack on public trust and confidence” and questioning the functionality of western democratic institutions (Spalding 2019). This misinformation was meant to target certain populations in the United States such as African-Americans, immigrants, far-right activists, and liberal thinkers. The main goal of targeting these groups was “to amplify an existing divide within the American public” (Spalding 2019) and create distrust in democratic institutions. An important impact of this misinformation campaign was that it allowed the United States to understand the critical role elections play in the country. Following the discovery of Russian interference in the 2016 election, the Obama administration designated the election infrastructure as a critical infrastructure subsector in the United States (Johnson 2017). By drawing larger attention to the election infrastructure, this designation is vital to protecting the United States’ election against misinformation in the future.

These types of misinformation campaigns are impactful for a variety of reasons, but two being the mistrust in America’s media and the use of social media as a means of receiving the news. In 2018, only 21% of Republicans stated they had “a great deal” or even “a fair amount” of trust in America's media (Jones 2018). This demonstrates the ability for right-wing citizens in the U.S. to not believe the mainstream media and become more likely to trust misinformation campaigns on social media. In addition to the mistrust in America's media, a large amount of Americans are receiving their news on social media platforms. In 2018, around 68% of Americans said they have used social media in some form to receive news (News Use Across Social Media Platforms 2018). This shift in using online platforms to receive news about the world is allowing misinformation to spread more easily and reach a larger array of people. Overall, misinformation campaigns create a large threat to geopolitics and relations between states, especially with the increased use of social media platforms.

## Security

### Challenges in Cybersecurity

One of the most important aspects of the digital domain is creating comprehensive cybersecurity policies to protect against cyber weapons. Compare to previous spaces in geopolitics, such as air, land, and sea, the digital domain creates more challenges in security. Governments across the globe are rapidly increasing security efforts to account for the threats in this shifting domain. Specifically, the United States increased funding by $800 billion for cyber defense in 2013 and the US Cyber Command will see an increase from 900 to 4,900 employees in the coming years (Douzet 2014). This rapid expansion and investment in cybersecurity demonstrate the increased risks to nations from cyberweapons. However, with a new domain being developed for geopolitics to exist in, there is also an increasing amount of issues with cybersecurity regulations.

**Case Study—European Union and Cybersecurity Challenges**

With recent developments in technology, cybersecurity is an important aspect of protecting societies against the harmful weapons in the digital domain. Since the cyber domain is a relatively unexplored territory for legislation, there is an opportunity to develop a sustainable framework for uniform cybersecurity regulations across countries. However, international organizations such as the European Union (EU) have struggled to create cohesive cybersecurity policies across their member-states for a variety of reasons (Fantin 2020).

First, many member-states in the EU see cybersecurity as impacting domestic policy and thus infringing on the sovereignty of the states (Fantin 2020). According to the United States, there are 16 critical sectors that will be impacted by cybersecurity regulations (Critical Infrastructure Sectors 2020). These sectors include a wide range of industries ranging from energy, to finance, to food and agriculture (Critical Infrastructure Sectors 2020). The diverse range of industries that are impacted by cybersecurity demonstrates how issues can arise in regulating a variety of sectors. There is then a repeat of a very common question within the EU, how can you protect the sovereignty of states while advancing security? This digital and political clash will continue to create issues in creating cohesive strategies for cybersecurity in the EU.

Additionally, similar to the United States, EU member-states are struggling to share cybersecurity strategies. Specifically, “given the sensitive nature of the technology, the sharing of capacities is perceived as giving up sovereignty and what it can reveal about strengths and weaknesses” (Douzet 2014). Not only is there a lack of transparency within the EU, but there are also significant disparities in the cyber tools developed by member-states. Throughout the EU, many experts have found “disparities in capabilities are very wide” with nations that have the “most advanced capabilities view them as an area of national sovereignty and give priority to cultivating bilateral arrangements" (Douzet 2014). In order to improve cybersecurity policies, the EU must follow the transparency of the United States in sharing its security policy.

Finally, there is a race for artificial intelligence across Europe which impacts the ability to create a cohesive cybersecurity strategy (Fantin 2020). There is a general sentiment that if you can be the first nation to master artificial intelligence, then you will dominate the geopolitical rise of this new technology (Fantin 2020). New developments in artificial intelligence will serve to shape political processes and relationships among powers (Technology Alliances Response to Geopolitical Tensions 2020). However, the competitive nature of artificial intelligence makes the EU member-states less inclined to regulate this market (Technology Alliances Response to Geopolitical Tensions 2020). Since European countries are not only in competition with each other but also are in competition with nations across the globe such as the United States and China, fewer governments are concerned with the security aspects of this technology and are more concerned with developing at a fast pace.

## Economics

### The Cost of Cybercrime

The digital domain is not only having an impact on the security of nation-states, but there are significant economic implications of cybercrime. In 2014, it was estimated that $445 billion was lost every year to cybercrime (Lewis 2018). By 2018, that number jumped to $600 billion, nearly one percent of global GDP (Lewis 2018). While hacking in a relatively cheap way to attack an adversary, costing as little as less than $100, there is often a large economic return. The financial gains from hacking generally come from the monetization of digital data, or creating ransomware attacks that ensure users will pay to retrieve their stolen data (Lewis 2018).

Specifically, the countries most impacted by cybercrime are the nations with higher a GDP or more advanced technological development, reflecting that "the richer the country, the greater its loss to cybercrime is likely to be" (Lewis 2018). Due to a larger amount of technological development, these nations are a larger target for cybercrime and consequently pay a larger price. In addition to the economic burden the digital domain creates for more developed countries, there are also differences in access to cyber tools between nations across the globe.

**The Digital Divide**

Since the rapid development of the digital domain, the creation of a digital divide has been introduced to nations. The digital divide represents how countries with varying economic resources are impacted differently to advancements in the digital domain. With a low barrier to entry and relatively low cost of resources, the digital domain shows some promise of allowing developing countries to participate in the technological rise (Dincic 2020). Specifically, the digital economy is able to include a variety of nations "by lowering transaction costs, addressing information asymmetries and exploiting economies of scale and network effects" (Dahlman, Mealy, and Wermelinger 2016). There are a variety of platforms and digital tools that are aiding the connectedness of developing countries to the digital domain, with one example being Ushahidi.

Ushahidi is an African software platform that looks to help victims in global emergencies. This platform is using technology to collect information at a high speed from the grassroots of African countries (Dincic 2020). The technology was originally developed in 2008 in Kenya following an increase in post-election violence to locate safe-havens for citizens (Ushahidi: The African Software Platform Helping Victims in Global Emergencies 2013).

However, the platform has expanded significantly to the Middle East and Asia to crowdsource information on violence and natural disasters (Ushahidi: The African Software Platform Helping Victims in Global Emergencies 2013). Ushahidi is a relevant example of how the developing world can utilize technology to advance the countries' connectedness and streamline effective communication.

There are also some challenges presenting in the engagement of the digital domain with developing countries. The digital divide can refer to the fact that many of the technological advancements occurring in developed countries "depend on a basic level of infrastructure that many emerging economies still lack" (Dahlman, Mealy, and Wermelinger 2016). It is estimated that "approximately two thirds of the world's population does not have access to the Internet. These 4.3 billion people generally live in rural, geographically dispersed areas" (Dahlman, Mealy, and Wermelinger 2016). Access to the internet is the more basic form of infrastructure needed to participate in the digital domain, but the majority of the world lacks internet connectivity. Even if developing countries are able to obtain this basic infrastructure, there will be a delay in their ability to implement these new technologies. This delay will allow developed countries to create the regulatory structure and form the digital frameworks for the globe, putting developing countries at a disadvantage (Dahlman, Mealy, and Wermelinger 2016). For this reason, it is recommended that developing countries "engage in strategic planning to maximise the development impact of digitalization" (Dahlman, Mealy, and Wermelinger 2016). If the developing world is to gain significantly from the digital domain, there needs to be a collaboration with the developed economies to ensure digital frameworks reflect the needs of all nations.

There are also some challenges for the developed world to engage with the digital domain. Specifically, in many OECD countries, there is significant growth in a select amount of large companies at the expense of smaller ones (Dincic 2020). These companies are creating monopolies on the technology market, especially with the increase in company mergers and buyouts that consolidate parts of the tech industry (Dahlman, Mealy, and Wermelinger 2016). Since these companies hold a significant share of the market concerning technological advancements, they have the ability to restrict government involvement in the development of the digital domain. However, there is hope for a public-private partnership in the United States with the expansion of the Defense Advanced Research Project Agency (DARPA). This institution serves "as a facilitator of knowledge-sharing and coordinator of research activities undertaken by various parties" which allows the federal government to promote advancement in developing technologies and encourage competition in the private sector (Dahlman, Mealy, and Wermelinger 2016). In funding initiatives such as DARPA, countries are able to decrease the hold large technology companies may have on the advancement of the digital domain.

## Conclusion

### The Future of Cyberwarfare

The digital domain is having a significant impact on geopolitics, specifically focusing on international security and geoeconomics. The vast amount of technological advances is creating new areas for adversaries to act, specifically exposing vulnerabilities in the digitization of energy and social media is allowing state and non-state actors to pursue misinformation campaigns. The example of the United States' power grid demonstrates how increasing digital tools in a country's infrastructure can leave states exposed to large cyber-attacks. Additionally, misinformation campaigns can weaken public confidence in federal institutions and create divisions between state populations. There are also large disparities in how nations are addressing the geoeconomic implications of the digital domain. In cyberspace, developing and developed countries are experiencing vast differences in access to digital tools and this could lead to gaps in who is positively impacted by the digital domain.

Overall, there are a variety of questions that remain unanswered with how nations will address the increasing geopolitical threat of the digital domain. Specifically, since the cyber domain is man-made unlike past spaces for geopolitics to exist, it is constantly changing and advancing. Without public-private partnerships between states and companies, federal governments and international organizations are not prepared to understand the rapid developments produced in the digital domain. Additionally, there are large gaps in securing the digital domain which could lead to vulnerabilities in international security. Countries need to create cohesive and collaborative cybersecurity regulation in order to combat the adversaries attempting to pursue cybercrimes. While the digital domain is advancing at a historic speed, nation-states may not be ready for the implications of cyberspace on geopolitics. The world is seeing a revolutionary shift in geopolitics and the "beginning of a growing period of dominance of cyberspace in international relations", but governments across the globe often lack the tools to effectively regulate this new domain (Popa 2014).

## Abbreviation List

SIT=School for International Training

EU=European Union

U.S.=United States

DARPA= Defense Advanced Research Project Agency

OECD=Organization for Economic Cooperation and Development

CSIS=Center for Strategic and International Studies

DoD=Department of Defense

## Bibliography

### Secondary Sources

(2001). “Air transport, passengers carried”. *The World Bank*. Retrieved from https://data.worldbank.org/indicator/IS.AIR.PSGR

(2014) “U.S. Risks National Blackout From Small-Scale Attack”. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/u-s-risks-national-blackout-from-small-scale-attack-1394664965?tesla=y

(2015). “Emerging Risk Series, Business Blackout”. *University of Cambridge*. Retrieved from https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-lloyds-business-blackout-scenario.pdf

(2018). “Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms”. *Council on Foreign Relations*. Retrieved from https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

(2018). “News Use Across Social Media Platforms 2018”. *Pew Research Center*. Retrieved from https://www.journalism.org/2018/09/10/news-use-across-social-media-platforms-2018/

(2018). “The Cost of Malicious Cyber Activity to the U.S. Economy”. *White House*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

(2019). “Our World in Data: Internet”. *Our World in Data*. Retrieved from https://ourworldindata.org/internet

(2019). “Report reveals play-by-play of first U.S. grid cyberattack”. *Energy Wire.* Retrieved from https://www.eenews.net/stories/1061111289

(2020). “Critical Infrastructure Sectors”. *Cybersecurity and Infrastructure Security Agency*. Retrieved from https://www.cisa.gov/critical-infrastructure-sectors

(2020). “Digital in 2020”. *We are Social*. Retrieved from https://wearesocial.com/digital-2020

Bussolati, N. (2014). “The Rise of Non-State Actors in Cyberwarfare”. *University of Amsterdam - Amsterdam Center for International Law*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2764185

Csurgai, G. (2019). “Geopolitical Analysis: A Multidimensional Approach to Analyze Power Rivalries in International Relations”.

Dahlman, D. & Mealy, S. & Wermelinger, M. (2016). “Harnessing the digital economy for developing countries”. *Organization for Economic Cooperation and Development (OECD).* Retrieved from https://www.oecd-ilibrary.org/docserver/4adffb24-en.pdf?expires=1587575022&id=id&accname=guest&checksum=CA0DFD8824AE2D2BEE1FC36BCA3081D5

Douzet, F. (2014). “La géopolitique pour comprendre le cyberspace”. *Hérodote*, no 152-153,(1), 3-21. Retrieved from https://www.cairn-int.info/article-E_HER_152_0003--understanding-cyberspace-with-geopolitic.htm

Friedman, F. (2016). “Seven hidden costs of a cyberattack”. *Deloitte*. Retrieved from https://www2.deloitte.com/us/en/pages/finance/articles/cfo-insights-seven-hidden-costs-cyberattack.html

Johnson, J. (2017). "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector". *Department of Homeland Security*. Retrieved from https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical

Jones, J. (2018). "U.S. Media Trust Continues to Recover From 2016 Low". *Gallup*. Retrieved from https://news.gallup.com/poll/243665/media-trust-continues-recover-2016-low.aspx

Lewis, J .(2018). "Economic Impact of Cybercrime". *Center for Strategic and International Studies.* Retrieved from https://www.csis.org/analysis/economic-impact-cybercrime

Popa, I. (2014). "Cyber Geopolitics And Sovereignty. An Introductory Overview". *The 5th International Scientific Conference.*

Spaulding, S. (2019). "Russia's Attacks On Democratic Justice Systems". *Center for Strategic and International Studies*. Retrieved from https://www.csis.org/features/russias-attacks-democratic-justice-systems

Tayouri, D. (2020). "The Secret War of Cyber Influence Operations and How to Identify Them". *Institute for National Security Studies (INSS)*. Retrieved from https://www.inss.org.il/wp-content/uploads/2020/03/Cyber4.1ENG_e-5-22.pdf

**Primary Sources**

(S. Fantin, personal communication, 02/24/2020)

(D. Dincic, personal communication, 04/14/2020)

(J. Duberry, personal communication, 4/20/2020)