The Enactment of a Strategy of Sanctions

Tristan Woodard
Old Dominion University
CYSE 425W Cyber Strategy and Policy
Professor Lora Pitman
October 16th, 2022

Cybersecurity has become a separate domain unto itself, where actors, at levels individual to global, act out scenes of conflict and warfare in the same manner as more traditional stages. This undertaking has long since passed, however, the importance of addressing and interacting with said domain will only grow with time as cyberspace develops further and grows even more in importance. With this being the case, nation states are forced into a situation where they must decide a course of action on how they will operate and behave within cyberspace, and in turn, be affected by the conflicts and events that occur both within cyberspace, and as a result of actions within cyberspace. With ambivalence not being an option, every nation must set forth specific policies and protocols on how to interact with cyberspace, whether it be a more passive, defensive, or even an active role. Of the many options and outcomes possible, many North Atlantic Treaty Organization (NATO) member states have chosen to enact a policy in which they will respond to certain perceived attacks from other non-member states with financial sanctions. In the following, I will outline the theoretical basis for why cyberspace is seen as a new domain in conflict between nations, and thus influenced the basis for such a policy stance. From there, I will outline the events in actuality that lead to the enactment of the policies, and then detail how exactly it was enacted within the NATO states that have enacted such a policy.

Within the realm of warfare, the United States (with many others subscribing to the same or similar stances) has defined four typical and kinetic domains of warfare(Fanelli, R., 2016). Those are Air, Land, Sea, and Space. Cyberspace, however, has now been specifically identified as the fifth domain of warfare. While certain principles and properties of this fifth domain are just the same as with other domains in warfare, most operate completely differently. By its very nature, cyberspace is a constantly changing, evolving, growing, shrinking, regrowing, and is a highly mutable field to operate in. This means that Information is paramount as opposed to a more traditional view of a combat domain where land control can be measured, or weaponry and manpower can be seen in real space in order to exert control over a location. This measure of success, control of information, can likely best be measured through use of the CIA Triad; confidentiality, integrity, and availability (Fanelli, R., 2016). To best explain this, imagine the following scenario. A local government office or business deep within the heart of country A is using its cyber technology and interacting with cyberspace on a daily basis. It makes money through cyberspace, maintains operations, established communications and links to outside organizations, and in a traditional view could surely be seen as being fully within the domain of country A in seemingly every aspect. However, if Country B effectively controls the aspects of the CIA triad (or even just one aspect), in all likelihood, Country A could not really be said to be in control of the information, and thus the office or business would be in actuality within the sphere of influence of Country B's cyberspace domain. This could be seen by imagining a scenario where all the transactions of the local office could be seen completely by an agent of Country B. This would clearly violate the confidentiality of the office's systems. Likewise, if Country B could simply block access to a number of systems to the office, it would violate the availability for those who rely on the office. So even though soldiers have not stormed the building, or double agents make up the administration of the office, in this scenario Country B has seemingly encapsulated the office within its domain, and not really within the domain of country A. This scenario and other's can paint a picture that would lead one to believe that traditional views on warfare and conflict may not translate so easily to the fifth domain of warfare. This could go a long way to explain just why measures seen as aggressive or offensive in nature, could be also described as defensive and reactive in the realm of cyberspace, when in other domains the opposite may be true (or at least able to be viewed as true). With this in mind, policymakers, administrators, tacticians, defense specialists, cyber specialists, and other professionals in charge of a nation's cyber defense and cyberwarfare strategy, may need to develop many new and/or novel ways to actively and effectively protect and defend their state's cyber domain. Such needs likely explain much of the backdrop for why certain measures were considered, or not considered by the United States and other NATO members, when cyber threats from non-NATO members were seemingly identified, and policy was drafted and enacted in order to respond.

While numerous cyberattacks have occurred over the years, from numerous sources, the Lazarus Group's attack on Sony Pictures Entertainment has been described as a “watershed moment” when it comes to events that lead to changes in policy towards cyber sanction strategy (Bartlett & Ophel, 2021). The Lazarus Group is identified as a cybercrime focused organization directly run by the Democratic People’s Republic of Korea (DPRK) (GULYÁS, 2022). Many point to the Lazarus group as the most blatant and cut and dry example of a state-sponsored agent of cyberwarfare. While they do serve a purpose of pursuing political matters, they are seemingly always performing attacks and actions with the aim of financial gain. Some of the attacks include the attack of Sony Pictures Entertainment in 2014 in response to a mocking film about the DPRK being made against the DPRK’s wishes by the company, the spread of the WannaCry ransom worm that infected over 300,000 computers, and numerous attacks on cryptocurrency systems that earned Lazarus upwards of 2 billion dollars. The Lazarus group has multiple subgroups and seemingly has ties to other nation states such as China and India. Another significant target of the United States. Cyber sanctions have been on Russia. The “watershed moment” in this case that led to significant shifts in policy towards cyber sanctions for Russia, would be the supposed interference in the 2016 American Presidential Elections, including the hack into the Democratic National Committee (DNC) (Bartlett & Ophel, 2021). Other Important cyberattacks that were attributed to Russia Include the 2017 NotPetya ransomware attack on Ukraine (which is not a NATO member themselves, but they are heavily tied to the NATO project, and a close partner), and the 2020 SolarWinds breach. The SolarWinds attack was notable for United States Intelligence and Policymakers, as it provided access to 18,000 computers, from private entities, all the way up to computers involved in high ranking state agencies like the department of the treasury, and the department of defense. While numerous entities in Russia have been accused of cybercrime and acts of cyberwarfare, many have pointed to the central security agency within Russia, the Federal Security Service (FSB), as being a large perpetrator of cyber crime. While the 2016 acts of supposed election interference were tied to the FSB, numerous other acts have also been brought forth as attributable to them. In 2018 and 2020 two Russian organizations were sanctioned due to allegations of providing the FSB with equipment that they used, or were intending to use, to intercept telecommunications sent across underwater cables. Further events attributed to the FSB include the 2007 Zeus malware, the 2011-14 Zeus botnet, the 2012-present Dridex Malware, the 2013 Cryptolocker Ransomware attacks, the 2014 Yahoo Hacks, among numerous others who were believed to have attempted to cover up or aid FSB operations or attacks (Bartlett & Ophel, 2021). Another important State to discuss when it comes to American and NATO cyber sanctions, is Iran. In fact, it may be argued that the first instances of cyber related sanctions occurred due to Iran's Minister of Intelligence's connections with Hezbollah (Bartlett & Ophel, 2021). Many other cyber related sanctions against Iran are aimed at the Islamic Revolutionary Guards Corps, an organization tasked with defending Iran in numerous ways, including cyber defense, Iranian Law Enforcement, Islamic Republic of Iran Broadcasting (IRIB), the Iranian Communications Regulatory Authority (CRA), Iran Electronics Industries (IEI), and Datak Telecom, and Iranian Internet Service Provider (ISP) (Starr, J., & Ighani, H., 2014). The Iranian Ministry of Intelligence has been accused of monitoring opposition groups, and general human rights abuses. Iranian Law Enforcement was accused of using technology to monitor dissidents, bloggers, and activists in order to facilitate and make arrests following elections such as the 2009 Iranian Election. Datak Telecom was accused of providing data to the Iranian Government in order to monitor email and facilitate arrests. IEI, IRIB, and the CRA were accused of denying a free flow of information to the Iranian people, with IEI being singled out for providing advanced eavesdropping, monitoring, and jamming tools (Starr, J., & Ighani, H., 2014). These three countries, the DPRK (with 18), Russia (with 141), and Iran (with 112), account for about 88% of the cyber related sanctions the United States has levied between 2011 and 2021, which is 311 sanctions in total. Other Countries represented in that remaining 12% are Pakistan at 11, Nigeria at 6, China at 5, Finland at 4, Syria and the Seychelles at 3, and Ukraine, Slovakia, Syria, the Central African Republic, and Sudan with less than 3 (Bartlett & Ophel, 2021). It is important to note that attributing actions and events to specific entities, states, and individuals is difficult. With situations like the Iranian Ministry of Intelligence, it is clear that those within the Ministry are operating on behalf of the state of Iran itself. While the only sanction levied at a Slovakian entity, were levied at an entity that seemingly was just trying to circumvent the sanctions and do business with one of the Russian entities that was supplying the FSB with equipment (US Treasury Dept, 2018). In that case, it likely could be argued the state of Slovakia itself was not actively targeting the United States, NATO, or other states through cyberwarfare. All these events provide a solid backdrop to explain what actions could be pointed to by policymakers as being significant and influential in the enactment of sanctions and development of further sanctioning policy.

As stated previously, from 2011 to 2021 there were a total of 311 sanctions enacted by the United States due to cyber related reasons (Bartlett & Ophel, 2021). These Sanctions mostly all came into existence through the enactment of two Executive Orders (EOs). EO 13694 was first passed by President Obama (Exec. Order No. 13694, 2015). It was largely thought to be a response to alleged Russian activity outlined previously (Bartlett & Ophel, 2021). The EO was amended later on in December 2016 after the 2016 United States Presidential Elections, to broaden the scope of the original EO (Bartlett & Ophel, 2021). This amendment, EO 13757, now included the ability to impose sanctions as a result of information based warfare, in cases where tampering or misappropriation of data is being used to undermine election integrity (Exec. Order No. 13757, 2016). The European Union (EU), not far behind, jointly established a framework in 2017 commonly called the "Cyber Diplomacy Toolbox"(EU External Action, 2020). It largely follows the same general principles as the United States response, however it should be noted the actual enacting of sanctions by the EU has happened far less often (Callo-Müller & Bogdanova, 2022). In 2019 the "The EU framework for restrictive measures against cyber-attacks threatening the EU and its member states" was put through. It was officially detailed in EU Council Regulation 2019/796 of 17 May 2019 (EU COUNCIL DECISION (CFSP) 2020/1127). Eventually, the first cyber sanctions against Russia were enacted using this framework (Callo-Müller & Bogdanova, 2022). A NATO member, former EU member, and close ally to the United States, The United Kingdom (U.K.), also put forth its own cyber sanctions policy after it exited the EU, called "The Cyber (Sanctions) (EU Exit) Regulations 2020" (Callo-Müller & Bogdanova, 2022). As of 2022, the U.K. has enacted cyber sanctions largely against Russian entities and persons, with smaller amounts at nationals/entities from China and The Democratic People's Republic of Korea (Gov.uk, 2022). While they are not a NATO or EU member, another closely related cyber sanction framework was enacted by Australia via the Autonomous Sanctions Amendment (Magnitsky-style and Other Thematic Sanctions) Bill 2021 (Callo-Müller & Bogdanova, 2022). All these sanction schemes allow countries to pursue the traditional outcomes associated with sanction tactics. This mostly involves the attempted change of a policy on the target end of the sanctions, often due to the pressure being applied to political leaders, and the populace as a whole (Iftimie, I., 2020).

In conclusion, the world has been put into a scenario where cyberwarfare and cyber-attacks have constituted a fifth domain of warfare that must be addressed. NATO member countries are no exception, and a few sets of policy have been enacted among them. NATO member states largely have seen Russia, Russian Entities, and Russian Nationals as the primary target of economic sanctions due to cyber activity. Within NATO member states, the United States, the EU, and the U.K. so far have been the ones to enact the most significant sanctions for cyber crimes, and have created the most comprehensive cyber sanctions policies within NATO. New sanctions, new amendments, and new strategies are being implemented to the present, and new dynamic strategies will likely continue to be necessary as nations react to and act within the fifth domain of warfare.

References

Iftimie, I. (2020). Cyber Sanctions: Weaponizing the Embargo of Flagged Data in a Fragmented Internet. Journal of Information Warfare, 19(1), 48–61. https://www.jstor.org/stable/27033608

Bartlett, J., & Ophel, M. (2021, May 4). Sanctions by the Numbers: Spotlight on Cyber Sanctions. Center for a New American Security. Retrieved October 16, 2022, from https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber

European Union External Action. (2020, July 30). EU imposes first ever cyber sanctions to protect itself from cyber-attacks. EU imposes first ever cyber sanctions to protect itself from cyber-attacks | EEAS Website. Retrieved October 16, 2022, from https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en

Union for Foreign Affairs and Security Policy, COUNCIL DECISION (CFSP) 2020/1127 (2020). Official Journal of the European Union. Retrieved October 16, 2022, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN.

Treasury Targets Attempted Circumvention of Sanctions. (2018, August 21). Retrieved October 16, 2022, from https://home.treasury.gov/news/press-releases/sm462.

Starr, J., & Ighani, H. (2014). Timeline of US sanctions. Iran Primer. Retrieved October 16, 2022, fromhttps://iranprimer.usip.org/sites/default/files/Sanctions%20Timeline_Starr%20and%20Ighani_US%20Feb%202016.pdf.

GULYÁS, A. (2022). “lazarus” the north korean hacker group. STRATEGIES XXI: The Complex and Dynamic Nature of the Security Environment, 75–83. https://doi.org/10.53477/2668-6511-22-08

Fanelli, R. (2016). Cyberspace Offense and Defense. Journal of Information Warfare, 15(2), 53–65. https://www.jstor.org/stable/26487531

Exec. Order No. 13694 (April 01, 2015)

Exec. Order No. 13757 (December 28, 2016)

Callo-Müller, M. V., & Bogdanova, I. (2022, January 24). Unilateral cyber sanctions and global cybersecurity law-making. Opinio Juris. Retrieved October 16, 2022, from http://opiniojuris.org/2022/01/24/unilateral-cyber-sanctions-and-global-cybersecurity-law-making/

CONSOLIDATED LIST OF FINANCIAL SANCTIONS TARGETS IN THE UK. (2022, May 7). Gov.uk. Retrieved October 16, 2022, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1088191/Cyber.pdf.