# Cyber Sanctions in Practice

Tristan Woodard

Old Dominion University

CYSE 425W Cyber Strategy and Policy

Professor Lora Pitman

November 6, 2022

The choice to pursue a policy where a host country issues and maintains a set of sanctions towards a target individual or entity, is a clear political maneuver with intentions and thought behind it. It is not the only option, nor is it par for the course for a diplomatic response. Nevertheless, such actions have been taken by numerous entities in the past decade, in an effort to combat and respond to cyberattacks and incidents. Of particular note are the numerous sanctions put forth by members of the North Atlantic Treaty Organization (NATO) against Non-NATO members. In the following paper I will detail what measures were taken by NATO member states to pursue a sanctions scheme against non-member states, why these specific measures were taken, and some of the ramifications and effects of the measures taken.

NATO members have broadly fallen into two camps when it comes to cyber sanctions, the United States (U.S.) enacted sanctions, and the European Union (EU) enacted sanctions. The United Kingdom (U.K.) and other NATO members with close ties to the EU such as Iceland and Norway, while not in the EU themselves, have broadly aligned their cyber sanctions frameworks to align themselves with EU sanctions (Thompson, 2021). The policy of employing cyber sanctions in the U.S. started in earnest in 2015 with Executive Order 13687 and was amended the same year with Executive Order 13694 (Rusinova et al.,

2020). It was further amended in 2016 due to changes in circumstance. The policy was further codified and developed with the passing of the Countering America's Adversaries Through Sanctions Act (CAATSA) of 2017. While originally very broad in scope and definition, the further acts and bills would provide more details on what sanctions could be pursued, as well as what government bodies would be involved in enacting the sanctions. The EU sanctions came later, broadly through the council decision of the EU Regulation of 17 May 2019. Before that point, a Cyber Diplomacy Toolbox was set out in 2017, but it did not see any significant use until the legally binding Regulation in 2019 established a clear set of measures on how to implement the policy. The schemes set forth by the U.S. and EU have numerous traits in common. Firstly, both sets of sanctions take both economic and political measures (van der Meer, 2018). Economic sanctions can be seen as relating to transactions and flow of goods. This often means that the target of the sanctions cannot do business within the host country in any capacity. Political sanctions are more broad in scope but could be, for example, blocking travel through a host countryva, or politically blacklisting an entity or person from conducting international business even outside the host country of the sanctions. Both the U.S. and EU sanction schemes are also referred to as “smart sanctions” as opposed to a “comprehensive sanction” scheme (Rusinova et al., 2020). This means the sanctions often target specific entities, individuals, and are often targeted in some way towards a particular method of achieving a goal. This would mean, for instance, a business could face means designed to affect operational costs, while an individual may face a targeted method designed to affect the individual specifically. A more comprehensive measure would be blacklisting an entire target country or an entire industry from any and all transactions, for instance. There are of course also numerous differences between the U.S. and EU measures. In general, the EU measures tend to be more based on democratic consensus, and require more oversight, careful measures, and possible justification. In general, the U.S. measures

tend to have less oversight, be much easier and quicker to implement, and require much less political capital to enact and maintain. The EU sanctions can be divided into three distinct categories (Bannelier et al., 2019). UN mandated sanctions receive justification and democratic consensus from the UN, and are enacted based on UN measures. Supplementary sanctions are not mandated by the UN, but are based on UN measures, and can be seen as UN policy taken further out. Autonomous sanctions are not based on any UN measure or mandate, and are instead enacted purely from EU measures and policy. Even more important than categorization of sanctions is how the sanctions are enacted. Implementation of EU sanctions are entirely derived upon the delisting and listing of sanction targets by the Unanimous Action taken by the EU Council (Rusinova et al., 2020). This unanimity requirement, while lauded as a clear sign of democratic practice and diplomatic cooperation, does require much more time and political effort to be spent in the enactment of any and all sanctions. The EU sanction scheme also importantly defines that a cyberattack that can result in sanctions must be something that has or would have a significant effect on a member state's critical infrastructure, defense, or another critical state function. Another important trait of the EU scheme is the requirement that the sanction list must be reviewed at least annually. In contrast, the U.S. seemingly only requires the president to enact said sanctions. Not only that, but the definition of an actionable cyberattack is more broad, being defined as simply breaching the cybersecurity of a U.S. entity, or even just being connected to an entity that does or has.

An important step to consider in the implementation of these cyber sanctions schemes, is why did the policy crafters and leaders of the schemes choose to implement what they did. The first and most obvious factor is the number of cyber incidents post-2010 by state and non-state actors, coupled with the rise of cyberspace as an important domain for state actors to protect and utilize. This, however, is mostly an intuitive process to understand.

If country A attacks an important asset of Country B, it will respond if it has the ability to do so. More difficult to assess, is the question of why did policymakers choose the specific implementations they did as opposed to any other one. One helpful pathway to bringing forth knowledge as to why, could be to look at other potential policies or responses that could have been enacted instead of a cyber sanctions scheme. One avenue would simply be to publically acquiesce to a cyber incident, and use the event as a catalyst to improve cyber defenses (van der Meer, 2018). This avenue on the surface may seem like an impossibility, however, the U.S. itself has enacted it before. In 2015 the U.S. government was attacked with the personal data of over 20 million entities being compromised. While U.S. intelligence believed China to be the most likely culprit, the U.S. chose to publicly acknowledge a lack of adequate cybersecurity measures, using the incident as a pathway to further bolster cyber-defenses. Eventually, only 1 Chinese National ever faced any legal consequence for the incident. This avenue likely has the best use case if the threat it faces is immense, or even stemming from a more powerful opponent, with no other clear pathway for resolution. In this instance, there was likely no pathway harming the Chinese Government, or any associated entities, and the failure of U.S. defense was so large that any diplomatic action may backfire. This avenue provides the benefit of not escalating conflict further, and perhaps even bringing awareness or political capital towards the bolstering of defenses. Another avenue one could take is the attempted staging of diplomatic protest. Diplomatic protests can often be either internally focused or done through an external entity. External entities could include options like the United Nations. An internally focused protest often includes the expelling of diplomats. This option has pros and cons. If successful, especially through an external entity, it could result in a huge bonus for international and domestic opinion of the incident. Such a result could lead to further diplomatic actions with more impactful results. If unsuccessful, though, there is hardly any downside. Expelled diplomats or motions in the UN, while diplomatically

significant, rarely ever lead to any significant rise in aggression or escalation. The cons are that overall it seems like a low risk but low reward move. Even in the best case scenario, where a recognized international entity like the UN approves of the diplomatic protest, it often would not, or could not lead to any significant repercussion for a target country. Without an international entity providing support, the diplomatic "rewards" would be even more miniscule. This leads to this avenue of action being often seen as ineffective. Another potential avenue is the pursuit of a legal measure against a target. Legal measures by their very nature often can only be enacted at a national level. This leads to this avenue being potentially more rewarding than a simple diplomatic protest, but also more risky as well. Pursuing a legal action often leads to the same international reputational damage as a diplomatic protest might. This could also act as a deterrent to some, especially those who may have business or political goals in the host country. If an individual could even potentially stand trial, it could even lead to a conviction, which would have a mountain of rewards for the host country. However, as it stands, almost every legal action in response to cyber incidents, fails to ever lead to any jail time or in person trial of any kind. Often even before charges, most entities that commit cyber crimes worthy of sanction or international criminal charges, rarely ever travel to any country they are involved in attacking. This makes the chance of seeing any actual legal repercussions practically zero. Another potential risk of this avenue is that if a proper set of legal charges are to be brought forth, such a trial or event could lead to exposed intelligence in order to supply proper judicial evidence worthy of a fair and proper trial. In this case, one could either play fast and loose and not collect any of the reputational benefits of the trial, or expose intelligence in order to make sure a proper court case or motion occurs. This avenue also has a much easier time leading to an escalation. Legal cases could be easily mocked up or brought forth against entities tied to the host country within the target country, as a direct response. Overall, this avenue could be seen as

low reward and low to medium risk. Other avenues could also be used that are not as diplomatic in nature. The two possible outcomes that are most likely in that case then would be a direct military response or a cyber operations response. While these both are much more direct and could result in potentially the highest level of reward, they also harbor by far the most amount of risk. Direct military action can be all but ruled out in most circumstances, as it provides astronomical risk in terms of political backlash, reputational damage, monetary and logistics damage, and a dramatic increase in potential for escalation. A cyber operation is similar in nature, but less so in all aspects. Most often these avenues are either not taken entirely, or only explored in extremely limited circumstances when the situation allows. Overall, this provides a background as to why sanctions may be employed by nations as opposed to other options. The more diplomatic options such as acquiescence, diplomatic protest, and legal charges all have limited use cases, and while providing small amounts of risk, often provide miniscule to no reward. More direct actions often produce considerable to extreme levels of risk, even if they provide a potentially stronger possible reward. This leaves cyber sanctions to be seen as a potential option to some. It provides some level of risk involved, especially when compared to the more trivial diplomatic efforts discussed. It also, however, does provide a larger potential gain than most diplomatic actions, without the potential catastrophic levels of risk associated with direct actions and intervention.

To gain a clearer full picture of the policy of economic sanctions as a response to cyberattacks and incidents by NATO members against non-member states, one should take the information available on what steps were taken, and why, and measure it against what the ramifications were from those policies. Firstly, the more theoretical and abstract consequences should be understood. An important part of that is to see what all such sanctions policies have not seemingly accomplished. Often, economic sanctions may be thought of as a potential path to shifting the course of a certain state's foreign or domestic

policy (Thompson, 2021). The absolute pinnacle of such goals would likely be outright regime change itself. So far, none of the aforementioned sanctions or sanction schemes have seemingly led to any large scale shifts in state policy, much less regime change. Not all hope is lost for those who view sanctions as an effective tool to change policy, however, as it may seem to at least play some part in effecting a more modest set of changes to occur in the political realm. These changes usually manifest in two distinct ways: constraints placed upon the target country, and the relaying of clear signals sent to numerous parties due to the policies. Firstly, constraints may be placed on a country due to these sanctions. If a country does look to expand its influence or accomplish goals using cyberattacks or cyber warfare, it becomes much less tenable as a useful policy when a target country is already at target of sanctions. When already constrained in such a way, international reputational damage could much more easily occur, making it much more difficult for the target country to easily achieve its goals using said methods. Signaling can come in a variety of ways. First off, it can play to domestic audiences for both the target country and host country of the sanctions. The host country can leverage the sanctions to garner more support for diplomatic efforts, or at the very least, sour opinion of a target country. Conversely, the target country may see support diminish as internationally recognized sanctions may harm the dealings and business of citizens or nationals within the target country. It also signals to allied states that the target country is a threat, enemy, or problem of some sort, allowing this signal to focus international allied attention towards combating the target. These theoretical impacts should be combined with the more grounded and material impacts to get a wider view of the effectiveness and consequences of the sanctions. This however does make things difficult for scrupulous observers, as in many cases the exact effectiveness of the sanctions is left up in the air. In the U.S. for instance, attempts by onlookers to extract answers from the government on how effective U.S. cyber sanctions have been met with at best generalities proclaiming them to be

broadly very effective, or at worst dodges the question entirely. It could be posited that one metric that could be used to more decisively view the direct results of the effectiveness of the policies' deterrence, is a figure such as the percentage increase of cost to commit a cyberattack by a target country. Such figures however, due to their very nature, are kept highly secret due to their sensitivity. Another potential avenue then could be to measure the costs of financial transactions that have been blocked by the financial sanctions. These financial data points, even if they were available, may not actually be the best metric to use. Due to the nature of the cyberattacks, where political and financial goals are melded in a web of inseparable connectivity, these figures may still not paint a full picture. Luckily, there are some data points out there that can at least provide some glance into the political implications of some of the sanctions implemented. Certain agencies like the Government Accountability Office (GAO), the Treasury's Office of Intelligence and Analysis (OIA), and the State Department's Bureau of Intelligence and Research have performed analyses of the U.S. sanctions. These reports however make an important distinction, being the difference between effectiveness, and impact. Impact can be seen as an analysis of the observed effects in a more narrow sense, while effectiveness is how the schemes are actually functioning in regard to meeting the long term policy goals set out by the U.S. Overall, it seems the GAO assessment may point towards an interesting result. While the available data seemed to show there was indeed a large economic impact, the eventual effectiveness may be in question (Government Accountability Office, 2019). This is due to the fact that while it seems a larger economic impact from a sanction may be more coercive in achieving intended outcomes, it also seems to be producing more unintended consequences. For instance, it seems that some of the studies are pointing to the notion that sanctions are causing a negative impact on public health, women's rights, democratic freedoms, and other human rights issues within the target countries. Not only that, but a more sizable economic impact seems to be associated with a

larger chance a target country will seek to decouple itself from American business, commercial trade, and financial and political ties, instead looking elsewhere, perhaps even towards rival states. This draws into question whether even successful economic sanctions with large scale success at causing economic damage will even be able to actually be effective at achieving long term political goals, and adequately meeting the goals the original policy behind the actions aims to meet. When looking at states most targeted by U.S. and EU sanctions, this data seems to track. Currently, there is no regime change in places such as The Russian Republic, The Islamic Republic of Iran, or the Democratic People's Republic of Korea due to U.S. or EU sanctions. Not only that, but the data suggesting that target states are more likely to turn away from sanctioning countries' finance and trade, is backed up considerably when considering those three primary targets.

In conclusion, the policy of NATO member states implementing sanctions against non-member states due to cyberattacks or incidents is a measured and deliberate policy choice with immense strategy behind such a choice. Said choice has been weighed against other diplomatic actions, and given the current landscape, it has likely been seen as a preferred option to take as it doesn't demand immense risk, but is also thought to bring a wide range of potential benefits. This policy was set in place in different ways within the EU and US, with a set of pros and cons to each implementation. Despite this, they both share a common set of concerns. With the limited data we do have for this highly classified field, it does seem that widely they do have some significant economic impact. Despite that however, numerous concerns arise as to the overall effectiveness of the policy itself in achieving its intended political goals. Paradoxically, in fact, it seems that the more efficient it actually works to make any economic impact as it is crafted to do, it also seems to cause many more latent consequences that could derail and harm the eventual effectiveness of the ability for the sanctions to truly meet the underlying aims behind them.

## References

Bannelier, K., Bozhkov, N., Delerue, F., Giumelli, F., Moret, E., & Van Horenbeeck, M. (2019). SPACE EXPLORATION: Mapping the EU's cyber sanctions regime. In P. Pawlak & T. Biersteker (Eds.), GUARDIAN OF THE GALAXY: EU cyber sanctions and norms in cyberspace (pp. 33–42). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21136.7

Government Accountability Office, GAO-20-145 (2019). Retrieved November 6, 2022, from https://www.gao.gov/products/gao-20-145.

Rusinova, V., Martynova, E., & Kurakina, P. (2020). Fighting cyber-attacks with sanctions: New threats, old responses. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3742751

Thompson, N. (2021). Countering malicious cyber activity: Targeted financial sanctions. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3770816

van der Meer, S. (2018). State-level responses to massive cyber-attacks: a policy toolbox. Clingendael Institute. http://www.jstor.org/stable/resrep21308