Cyber-Sanctions Policy: Why, What's Happened, and What Else

Tristan Woodard

Old Dominion University

CYSE 425W Cyber Strategy and Policy

Professor Lora Pitman

December 4, 2022

At times when policy is discussed, a common scenario that plays out is that a large amount of the factors that played into the policy's development and implementation are stripped away. At times, it can be easy to try to boil down important and far-reaching policies into purely utilitarian or economic realms of discussion. Many other factors can be made to be subservient or undiscussed in comparison. This can be a grave mistake if one were to attempt to properly diagnose and understand the policy, though. Even if economic factors are often massively influential, and even if a utilitarian analysis can be helpful in some ways, they are not the only, or even primary methods with which one can interact with a policy, its development, and its effects. A businessman who is implementing policy to make money may attempt to implement policies that, on paper, lead to the most profit. This same businessman would likely often be met with trouble, as without considering the vast amount of social and societal factors at play, one could not reasonably hope to implement proper policy to reach a desired goal. Cyber policy is absolutely no different. While certain actors may wish to implement the "best" policy on paper that provides the "most security", such sentiments are short-sighted, as a vast array of social factors are in play that make such a goal unattainable in the first place. Most policymakers and leaders know this all too well, and as

such, many attempted to include those factors in the decision-making process when creating and implementing policy. The strategy of cyber sanctions by members of the North Atlantic Treaty Organization (NATO) and the European Union (EU), is no different. In the following paper, I will delve into the social and societal factors that likely lead to the initial developments of the aforementioned policy, the social consequences that arose from that policy, and other potential paths that could be implemented that may interact with the societal and social influences in different ways.

There were many social factors that led to the current initial developments of the modern EU and NATO policy of sanctions for cyber related issues. The most commonly cited catalyst seems to be the more advanced Russian cyberattacks, but especially the 2016 NotPetya attack attributed to the Russian state (Shea 2017). Almost all of that attack was targeted against Ukraine, particularly Ukrainian critical infrastructure. Both the EU, NATO, and The United States (U.S.) have interests in Ukraine, despite it not being a member of either NATO or the EU. This fact, combined with the real world infrastructure damage (not just damages some see as being purely in cyberspace), caused a lot of concern and influenced decision-making immensely. Often many western countries, but especially the U.S., have been seen as working as a risk based society, or risk based state (Kaminska 2021). Often, measured and calculated responses are put forth in response to any sort of new circumstance or necessary impending change. This has caused the U.S., its NATO Allies, and its close partners in the EU to all take very calculated steps in response to perceived threats. Cyberattacks are even more subject to this pattern, and while there are a multitude of reasons, two particularly stand out. Firstly, cyberspace is unlike any other domain of warfare, it is new, highly complex, and subject to misinformation, misunderstanding, and unintended effects even more so than other domains. Secondly, proliferation of cyber weapons and methods are on a different level when compared to traditional weaponry. The ease in which

malware, or a botnet can be misused, re-appropriated, reverse engineered, and redeployed is far greater than traditional weaponry. If a state were to be too aggressive with its cyber-weaponry and capabilities, it may risk massive collateral damage, or cyber-armaments falling into the hands of its most bitter rivals. With these factors in mind, one may start to truly see the complex needs at hand that must be addressed with a cyber policy from two of the most influential supranational organizations in the world. The growing cyber threat and perceived encroachment of Russian cyberattacks, especially on key allies, was begging to be addressed. Meanwhile, the need for a risk based assessment and measured response was still looming as intensely as it had ever been. This is in part why specifically the sanction's strategy was taken instead of others.

One of the first societal consequences that could result from the policy, is its effects on law enforcement (Bannelier et al., 2019). Firstly, more strain and workload are placed on all levels of law enforcement. While of course a cyberspace related unit will have more responsibility, other units will also face more difficulty, as subjects may need to be physically apprehended, areas be secured, international and domestic travel disrupted and secured, among many other duties. This can lead to a number of different latent consequences, including the raising of the difficulty for law enforcement to properly complete other duties, as well as a potential ballooning in police bureaucracy and police presence in lawful citizen's daily lives. Another societal consequence is the potential breakdown of international relations, or escalations of tensions. Cyber criminals that operate on an international level can only be caught or punished if multiple national entities work together. Such cyber sanctions against nationals from foreign countries may then cause a breakdown of foreign relations, or, at best, an escalation of tensions. Even if wrongdoing can be proven, cooperation can still require resources on all sides, which some states may not wish to give up. Overall, the real world effects can lead to further escalations in tensions, travel restrictions between countries,

diplomats being recalled, or potentially even real bloodshed or conflict. Another real world and societal consequence of sanctions is a potential pivot towards cryptocurrency usage to circumvent sanctions. The full scale of which states or entities are evading sanctions using cryptocurrency, and how, is not fully known. The U.S. has claimed that Iran is likely to be doing so, and has made similar claims about the Democratic People's Republic of Korea, The Russian Republic, and Venezuela. Cryptocurrency has had many attributed negative consequences, but its future proliferation of use could only lead to more societal consequences if its usage is seen as a viable path to evading sanctions. As of 2018 the EU had not taken any direct steps to combat usage of cryptocurrency, and instead devolved the matter to individual member states. The U.S. meanwhile had already issued some executive orders to combat use of cryptocurrency to circumvent sanctions, particularly levied at Venezuela.

With many of the underlying societal and social issues that caused the policy to come into place as a backdrop, and the potential and current societal consequences also in mind, one would then likely wonder what other potential routes could be taken that address the underlying issues, while perhaps leading to different outcomes. One possible route that could be taken, is not to implement sanctions, but to instead attempt to de-escalate, and harden defenses instead (Kaminska 2021). If an attempted attack doesn't even pose a significant threat to the defender, it's very easy to de-escalate tensions and continue normal operations. This strategy has actually often been a preferred strategy of the United States in many matters, however, it can often be hard to justify. When attacks are targeted against key allies, there will likely be intense social and political pressure by those allies and their interest groups to respond in some way. Justifying the strengthening of domestic cyber defenses can often come without much difficulty, but strengthening of an ally's defenses may come with blowback. In this case, a more aggressive option may seem to be the most politically feasible option. De-escalation is also very difficult in the realm of cyberspace (Lin 2012). With the

realm of cyberspace being much more mutable and unclear than a conventional domain of war, it is often impossible for certain leaders to be fully trusting that a mutual de-escalation is taking place. A “cyber-cease fire” is especially difficult to implement, and with mounting social and political pressure on both sides, it is often calculated that it is in the best interest of most combatants to continue some sort of offensive in some way. So de-escalation tactics, while beneficial for many, could be seen as politically difficult, taking a lot of restraint and level-headed crisis stability to enact. Another potential avenue is the implementation of a policy of Cyber Enhanced Sanctions (CES) (Peters 2017). CES are described as using a conventional sanctions strategy coupled with offensive cyber measures in order to support the implementation and follow through of the sanctions. This can involve numerous tactics to do so. For instance, if Country A is seen as using coercive measures against Country B, and Country C is an ally of Country B and wishes to see this coercion end, it could breach Country A’s cyber defenses, and have the assets supposedly siphoned from Country B returned. Websites associated with sanction targets could be attacked with DDoS or DoS attacks, rendering them unavailable. Assets could be frozen or re-appropriated worldwide or through third party means, not only just with banks and institutions in the host country. Malware could be injected, certificates forged, financial data could be made public, and even kinetic warfare could be disrupted through cyber means. This potential route would likely be much more effective at enforcing changes, and would answer many of the issues brought forth that the current policy is attempting to address. Likely allies would be satisfied at the increase in aggressiveness, and the insurance that sanctions will be enforced. Domestic backlash will likely be minimized and domestic rivals hindered, as the aggressive stance is likely to lead to effective propaganda and press at home. However, there are a litany of potential negatives as well. This method has the exact opposite advantages of a more subdued response intended for de-escalation. Legality is deeply in question with this method. Foreign

states and businesses may have negative views of the policy, which could cause economic and social unrest. Further escalation is likely, as is proliferation of cyber warfare armaments. Political polarization is also more likely to occur, especially across countries, as travel would likely see more restrictions, and the risk of an armed conflict would increase.

In conclusion, there are a number of social and societal factors that lead to the current policy of cyber sanctions. The wish for NATO and the EU to protect its international interests within allied neighbors, combined with domestic clammerings for tougher actions, led to the ability to enact an aggressive policy stance. However, due to the risk based nature of the member states, and a calculated and measured response to perceived threats, the response was both more aggressive than proponents of de-escalation and more crisis stability would prefer, but not as aggressive as a potentially more domineering or jingoistic potential response. The current policy could be seeing potential results such as strain of law enforcement, breakdown of diplomatic relations, escalation of tensions, more travel restrictions, and even an increase in the likelihood of more kinetic warfare occurring worldwide. Among the many alternatives though, the most likely routes that could, or could have been taken, are a strategy of de-escalation coupled with cyber-hardening, or a more aggressive strategy based around CES.

References

Bannelier, K., Bozhkov, N., Delerue, F., Giumelli, F., Moret, E., & Van Horenbeeck, M. (2019). GALACTIC COLLISION: Cyber sanctions and real-world consequences. In P. Pawlak & T. Biersteker (Eds.), GUARDIAN OF THE GALAXY: EU cyber sanctions and norms in cyberspace (pp. 79–86). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21136.12

Lin, H. (2012). Escalation Dynamics and Conflict Termination in Cyberspace. Strategic Studies Quarterly, 6(3), 46–70. http://www.jstor.org/stable/26267261

Kaminska, M. (2021), Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. Journal of Cybersecurity, 7(1). https://doi.org/10.1093/cybsec/tyab008

Peters, M. (2017). Cyber Enhanced Sanction Strategies: Do Options Exist? Journal of Law & Cyber Warfare, 6(1), 95–154. http://www.jstor.org/stable/26441282

Shea, J. (2017). How is NATO Meeting the Challenge of Cyberspace? PRISM, 7(2), 18–29. http://www.jstor.org/stable/26470515