European Union policy and the use of the normative power regarding cybersecurity

Políticas de la Unión Europea y el uso del poder normativo en el ámbito de la ciberseguridad

Kondrotas, Lukas

Lukas Kondrotas ** Lukas.Kondrotas@e-campus.uab.cat
University of Barcelona, España

Análisis Jurídico – Político
Universidad Nacional Abierta y a Distancia, Colombia
ISSN: 2665-5470
ISSN-e: 2665-5489
Periodicity: Semestral
vol. 4, no. 7, 2022
revista.analisisjuridico@unad.edu.co

Received: 10 December 2021
Accepted: 25 January 2022

URL: http://portal.amelica.org/ameli/journal/702/7024233008/

Abstract: The transformation of our societies due to technological progress and worldwide spread of information technologies has established a new domain where states must establish a "normal" way of relating to each other. National legislation has been adapted in order to reach this domain; however, in an international context there are still different manners to interpret what behaviour is normal and acceptable. The European Union has established a framework regarding its own cybersecurity and aims to establish the rule-of-law to progress towards a secure digital world; it has also created sanction rules to punish behaviours which oppose its own view. This paper tries to look at what effects it has had on other major actors in the realm of cybersecurity: The United States, Russia, and China. By looking at the development of the frameworks of these countries and their actions and comparing it to the objectives of the European Union in this matter, it shows that effects have been different in each case and that they are not coercing the actions of the other states, not because of a failed implementation, but due to their own nature.

Keywords: China, cybersecurity, European Union, normative power, Russia, sanctions, United States.

Resumen: La transformación de nuestras sociedades a causa del progreso tecnológico y la expansión de las TIC a escala global ha creado un nuevo ámbito en el cual los estados deben establecer una nueva manera "normal" de relacionarse entre ellos. Para ello, se han adaptado legislaciones a nivel nacional; sin embargo, en el contexto internacional, existen maneras diferentes de interpretar la forma "normal" de relacionarse en este ámbito. La Unión Europea ha creado un marco para su propia ciberseguridad y espera expandir el estado de derecho para progresar hacia un mundo digital seguro. También ha establecido un marco de sanciones para luchar contra las actitudes que van en contra de su punto de vista. Este artículo intenta ver cómo ha afectado esto a los actores más importantes en el mundo de la ciberseguridad: Estados Unidos, Rusia y China. Se ve que los efectos han sido diferentes en cada caso y no son coercitivos para las acciones de los demás estados, pero no por un fracaso de implementación, sino por su propia naturaleza.

Palabras clave: China, ciberseguridad, Estados Unidos, poder normativo, Rusia, sanciones, Unión Europea.

1. Introduction

In this paper, we are going to analyse the European cybersecurity policy and the effects on the behaviour of other major states, namely the United States of America, China and Russia of this policy, to see whether the EU has been able or could be able to influence their actions via norms and identities. We are also going to look at restrictive measures (sanctions) when used as a foreign policy instrument in order to signal specific values by a state. Therefore, our objectives are mainly two: understand the policy in this domain and see whether other states have been influenced by it.

We will be seeking to answer two questions in this regard: What effects does the European policy have on an international level? Are sanctions in any way able to boost these effects? Can the European Union become a leader in the domain of cybersecurity?

The current hypothesis is that these policies do not have a significant effect on an international level. We are going to try to confirm or reject this by studying the variables of application of the cybersecurity framework, sanctions and the behaviour of other states in this regard.

Moreover, we are going to also focus on the creation of identities as part of partner/rival interactions, perceptions, and self-perceptions as key factors to understanding the development of these policies in all these cases.

The text is structured by introducing our objectives for this work, a conceptual framework regarding basic concepts from IR we are going to use, the comparison of cases and developments of the events in each of the countries we are going to look at, analysis of these cases by applying the theoretical framework and a brief conclusion to summarise all the contents we will be looking at.

2. Conceptual framework

For our analysis, we are going to introduce some key concepts and theories which will allow us to systemise our approach to the subject at hand.

2.1. Sanctions as a foreign policy instrument

2.1.1. Sanctions in the international community

Biersteker & Portela explain that there are three types of "embeddedness" of sanctions. All members of the United Nations are under the obligation to implement sanctions under Chapter VII of the UN Charter. The second type is "supplementary measures", EU autonomous sanctions to amplify the first type of sanctions, based on the wording of those measures. And finally, there are autonomous sanctions which do not supplement UN sanctions (normally because the UN was unable to agree on sanctions) but are used by the European Union to show its position on a particular issue (Biersteker & Portela, 2015).

Just as these sanctions have to be understood in a broader scope of action, supported by other measures (both negative and positive), alignment between likeminded states is normal. Many times, this is the case regarding the sanctions

imposed by the EU and the US. However, sometimes there are disagreements (for example, the sanctions on Cuba by the US and the extraterritorial conditions of these sanctions). The authors also state that the US "advocates for regime change", while "the EU tends to demand compliance from the target". In some cases, the EU sanctions come before the UN sanctions (Sudan, DRC and Yugoslavia) (Biersteker & Portela, 2015, p. 3).

2.1.2. Legal basis in the EU

Even though sanctions were enabled in 1957 with the Treaty of Rome, with the Maastricht Treaty, in 1992 the European Union began using sanctions as a political tool. Three documents are relevant to coordinate these sanctions: the "Basic Principles on the Use of Restrictive Measures (Sanctions)", the "Guidelines on Implementation and Evaluation of Restrictive Measures (Sanctions) in the framework of the EU Common Foreign and Security policy" and "The EU Best Practices for the Effective Implementation of Restrictive Measures".

Member states or the HR/VP, supported by the Commission, can start the process, regulated by Articles 30 and 31 of the Treaty of the European Union (Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, 2012).

2.1.3. How sanctions work

Traditionally, in political science, a widespread belief that sanctions do not work has been a key idea for many authors. However, some researchers have challenged this idea by deepening the perspective for the analysis. Instead of focusing on a "pain-gain" analysis, where correlation between sanctions and political power vis-à-vis other actors is considered the only or, at least, the most impor- tant axis, a deeper understanding of sanctions can be achieved by classifying them according to their purpose, their impact, and their feasibility (Giumelli, 2013, pp. 9-20).

Cases where the requests from the EU to the sanctioned actor are not likely to happen but have a significant impact on their gains calculation formula are constraining, as they increase the cost; those which are likely to be complied with and have an important impact on the calculation are for coercing purposes, as they aim to change the behaviour of an actor; finally, those which have a low impact, regardless of their feasibility (sometimes feasibility is irrelevant, as some sanctions do not send a direct political request to the actor), are for signalling purposes –they show the disapproval of the EU of the past behaviour of the target actor. Of course, these purposes sometimes may overlap. Most of these logics do not correspond to a coercing logic –as most of sanctions actually focus on constraining or signalling (Giumelli, 2013, p. 21).

For example, after the annexation of Crimea in 2014 by Russia, the EU adopted a wide variety of restrictive measures which had a strong economic impact on Russia, accepting the collateral damages of broader sanctions on individuals not related to the actions of the target. This was a change to the previous policy of very narrow, non-economic sanctions and it also challenged

the Russian Federation, something the European Union was unwilling to do before. This shows that the EU has socialised its members to get used to sanctions and they have become more daring in their measures (Portela, 2016a, pp. 36-41).

2.1.4. What are "targeted" sanctions?

As we have explained, the nature of sanctions has changed over time. Embargoes were very broad and had devastating effects on civilian populations unrelated to the decision-making processes, which lead to the improvement of sanctions towards "targeted sanctions", which meant that their effects were not as significant on society as a whole but particular wrongdoing individuals. This idea has also led to the hope that possible targets would take these sanctions into account, and it would allow sanctions to be more effective, by making them unnecessary in some cases (as decision-makers would take into account sanctions into their cost-benefit calculation) (Portela, 2016b, pp. 2-6).

> What justifies the inclusion of a particular measure in the targeted sanctions toolbox is its amenability to be targeted at a pre-determined group of individuals, entities or sectors. The critical quality distinguishing a smart sanction is that 'it is designed to hit at the interest of individuals or groups in positions of power directly, rather than the entity they control'. (Stenhammar, 2004, p. 150)

However, this trend towards targeted sanctions has been changing and broadening, as mentioned previously, probably to make the effects stronger. This is problematic as instruments to monitor the effectiveness of restrictive measures and improve international cooperation regarding the reasons being sanctioned have not developed. This means that the collateral damages have expanded, even though the EU has advocated its moral high ground when presenting these sanctions. Even the targeted sanctions have swayed towards other groups, which are not involved in the decision making (likely, supporters of the decision makers in mind) (Portela, 2016b, p. 15).

2.2. What is normal, anyway?

To understand the inner workings of normative power, we first must understand what norms are. "Norms are usually described as collective, intersubjectively shared expectations of appropriate behaviour for actors with a given identity." (Katzenstein, 1996, p. 5) Norms establish action patterns, which in turn are interpreted as either permitted or prohibited. This further develops the identities and their self-conception of the actors. Norms, however, are not static concepts, as much as processes which are elaborated, contested and intersubjectively decided by the subjects, meaning that at any moment previous norms might be reinterpreted and adapted for a specific situation. They affect these subjects as much as these subjects affect them. (Wunderlich, 2020, pp. 5-6) The norms are regular patterns which affect those pertaining to a group – creating expectations of reciprocity and establishing a sort of "scope of actions" the actors can choose from in a certain situation. These norms prescribe and proscribe behaviours, implying the "do's and don'ts". This, in result, legitimates one type of acts, those which are consistent with the patterns appropriate to the

type of actor, and "delegitimates" others, the ones which are not (Wunderlich, 2020, p. 16).

2.2.1. Hedley Bull, rules and institutions

In his International Relations classic, The Anarchical Society: A Study of Order in World Politics, Hedley Bull highlights that in order for rules to be socially implemented, institutions (both rules and institutions understood in a broad sense) must carry out some of the following functions: 1) the rules must be made; 2) they must be communicated; 3) they must be administered; 4) they have to be interpreted; 5) the rules need to be enforced, in order to be effective; 6) they have to be legitimised by those whom they apply to; 7) they have to be able to adapt to change; 8) and, finally, they have to be protected —by a system which itself guarantees the operation of the rules—. These rules do not have to emerge as laws, as they might emerge as common practices, which then, through a process, evolve into legal conventions agreed upon by the States. Finally, he understands that rules can be divided into categories, and the highlights three types of rules 1) Fundamental or constitutional normative principles; 2) Rules of coexistence; and 3) Rules which regulate cooperation (Bull, 1995, pp. 54-67).

2.2.2. Normative Power: Ian Manners

In his works, Ian Manners discusses the nature of what has been called "Normative Power", explaining that it is different from traditional power of the states. In "Normative power Europe: a contradiction in terms?", he argues that to understand events such as the collapse of the Communist regimes in Eastern Europe in the 1990s, we have to understand the power of ideas and norms. Manners bases his ideas on earlier thinkers, such as Carr, Duchêne and Galtung. These authors share the idea about the existence of a type of power which allows for the "power-sender" to change the ideas of the "power-recipient". Manners states that they, in some way, referred to this type of power in their work, even though they did not use that denomination. For Manners, both the European Union's civilians and military power "need to be augmented with a focus on normative power of an ideational nature characterized by common principles and willingness to disregard Westphalian conventions". Another key feature that he highlights, originating from Buzan and Little, is the uniqueness of the EU as an actor, as it is different from both pre-Westphalian political units and Westphalian ones, therefore it has certain unique characteristics and capacities (Manners, 2002, pp. 39-40).

The EU, for example, shapes its external relations based on ideas and principles, "based on its policy to consolidate democracy, rule of law, and respect for human rights and fundamental freedoms". Manners, however, denies that the use of military power to use force as an instrument to implement it —for the EU is a different type of actor, compared to a state (Manners, 2002, pp. 241-242).

3. Understanding the cybersecurity agenda of the European Union

3.1. Understanding cybersecurity

The EU has provided a wide variety of definitions for the usage of this term, as ENISA released a document about the standardisation of the definition, calling for use of the specific definitions provided and the three strands discussed in the document (Brookson et al., 2015, pp. 6-26).

3.2. Cybersecurity as part of the European Security Strategy

Even though it becomes part of the mainstream defence agenda, as cyberdefence, cybersecurity is considered in these texts as part of general security when discussing the topic. "A Secure Europe in a Better World. European Security Strategy" approved by the European Council in 2003, cybersecurity is not mentioned in this text; nonetheless, it "defines, sorts, contains, synthetises and expresses the interests and the approach taken by the European Union in the world to advance together towards a greater regional and global security and its consolidation in the world" (Fernandez Bermejo & Martinez Atienza, 2018, p. 57; translation by author).

In 2013, the EU published a document titled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace". It maintains that those values upheld by the European Union offline should also be upheld online. It also outlines the strategic priorities of the EU regarding this topic, those being:

1. Achieving cyber resilience
2. Drastically reducing cybercrime
3. Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
4. Develop the industrial and technological resources for cybersecurity
5. Establish a coherent international cyberspace policy for the European Union and promote core EU values (European Commission, 2013, pp. 4-5).

The text further develops how these topics should be approached and the objectives related to these priorities. To properly fulfil these duties, a coordination between organisations on the national and the EU level are to be coordinated, as national governments have their legislation but require collaboration from the European Union as the nature of these type of crimes can easily be international of transnational.

Some authors have claimed, regarding the question of global cybersecurity cooperation, that a position of power is earned either by "right or might", and if the EU wishes to become one, it will have to earn its place in the "big boys" league. Some member states, such as Germany or France are relatively important cybersecurity players; however, the Union as such is still a work-in-progress to become a big name. TEuropean Union, as a regional organization has some sui generis traits which allow it to avoid traditional power struggles and engage in multilateral dialogue with multiple actors (Renard, 2018, pp. 7-8).

3.3. European cybersecurity act

2013 was a key year in terms of European Security, as ENISA, the agency established in 2004 as a temporary agency to support the Commission and the Member States. In 2013, under the European Cybersecurity Act, it became a permanent agency with better funding as it had proved of great use and efficiency in the previous years. It then undertook a plan to establish a cooperation network in the EU by establishing Computer Emergency Response Teams (CERTs) and Computer Emergency Response Team - European Union (CERT-EU), made up of IT security experts working for the main EU institutions. The expansion and strengthening of ENISA gave it more leverage and responsibilities, as it became the main agency in terms of EU cybersecurity. In addition to supporting the Commission and the Member States, the ENISA was now in charge of deploying the cooperation strategy and European certification network in terms of cybersecurity. The Cybersecurity Act provided standards for voluntary certification which complied with EU-wide regulation, assuring producers that their products would be legal in all member states if they complied with the certification (unless additional certificates were needed). ENISA was also tasked with the responsibility regarding data breaches related to the General Data Protection Regulation (GDPR), created in 2016 in order to protect the data and privacy in the EU (Giustozzi, 2019).

3.4. The EU's Cybersecurity Strategy for the Digital Decade

In December of 2020, the European Commission released a joint communication where it stressed the reliance of the bloc on the digital media (especially stressed due to the COVID-19 pandemic, which allowed for a hastened transition to telework for many individuals (40% of EU workers). The joint communication is divided into an introduction, where current threats and transformation processes are explained; the European motto and an explanation for its cybersecurity strategy; a rundown of the high-priority targets for cyberattacks in the EU structure; a brief conclusion, and appendices with key steps for its cybersecurity.

The document highlighted the need for a rule based global cyberspace, where the values of the EU would be reflected. At the same time, it warned about the decentralised system on which the internet relies, while ironically, some key structures and infrastructures being run by very few private firms. The "lack of collective situational awareness of cyber threats" remained a key problem, as the directive regarding cooperation regarding the security of network and information systems is limited (Directive [EU] 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016).

The cybersecurity strategy is in line with the European external action strategy — "Thinking global, acting European" —, and it addressed three focus areas for EU action:

1. Resilience, technological sovereignty, and leadership

2. Building operational capacity to prevent, deter and respond
3. Advancing a global and open cyberspace.

These aspects are considered as a crucial part of democratic processes and institutions, which is the objective of the strategy (European Commission, 2020, pp. 1-4).

These ideas have come into conflict with the open-market policies, as securitization discourses have been applied to technologies such as the 5G networks developed in third countries (namely, China). Other concerns have been raised when talking about the safety of the Internet of Things (IoT) and the integrity of the global DNS root system and the introduction of other key internet standards (European Commission, 2020, pp. 8-12).

The EU has set itself to establishing its rule of law to be able to reach and deal with digital crime. In 2019, the EU introduced a "cyber diplomacy toolbox" to defend its network effectively and comprehensively from attacks by malicious agents. The HR/VP is set to promote a working group especially dedicated to cyber intelligence. All these efforts are aimed to "contribute to responsible state behaviour and cooperation in cyberspace and should give particular direction on countering those cyber-attacks that have the most significant effect, notably those affecting our critical infrastructure, democratic institutions and processes" (European Commission, 2020, pp. 16-17).

According to the communication, these technologies have to be "global, open, human-centric, privacy-focused, and their use lawful, safe and ethical". This also should translate on the state level, where their behaviour should be ruled by international law. These actions would create safer and safe communities and cybercommunities and would, in turn, allow greater cooperation. Finally, there is a need to engage with other regional organizations to make sure the same line of work is followed to boost the implementation of the Agenda (European Commission, 2020, pp. 20-22).

4. Responses to the European foreign policy related to cybersecurity

Due to the nature of the "arms race" between attackers and defenders, attackers have the upper hand thanks to the wider availability of vulnerabilities and the narrow, focused capacities used by the defenders. Starting in 2016, defenders have increased their knowledge on the modus operandi of the attackers to prepare themselves for possible future attacks by understanding their mindset.

Especially relevant for the topic at hand are the state sponsored actors. There was a breach of state-sponsored tools, the first one of its kind. This has worried many experts as they have posed the question of whether this kind of breach is similar to "a loss of heavy weapons" by a state actor. On top of the actual anonymization tendency already spotted amongst the attackers, state related actors make an even greater effort to mask their trail, make their attacks as similar to those of regular cybercriminals or actual companies have been contracted to make the dealings of a state-actor. "Cyber fighters" is also a term used in this report to refer to a group that mixes "activists, terrorists, cyber-spies and cyber-

army". Their ideological motivations make them extremely active in their efforts against their targets (ENISA, 2017, pp. 67-71).

In 2017, ENISA stated that threat masquerading has widely extended to the other actor groups; however, state-sponsored actors remained the most advanced ones in their techniques.

State-sponsored actors went from the fourth most important group to the third one that year. On top of that, due to the extra difficulty of attribution of attacks perpetrated by this group, their percentage share of attacks (identified as 20%) should be even greater than that. In fact, ENISA identified states as especially dangerous actors in this field due to their investment in the development of capabilities and the fact that this trend is increasing (ENISA, 2018, pp. 91-96).

A change in the state-sponsored actors was seen, as some traditional groups changed their activities, other groups took its place, using similar means to the previous group. Rising tensions between states (especially China and the US, but also others, such as Russia, Germany or the UK) lead to references to cybersecurity during 2018. It became clear that cybersecurity (or at least, cyberespionage) must be taken into account when considering traditional politics among nations. Analysing the decrease of activity of traditional state-sponsored cyberthreat groups might point to the fact that states are reorganising their capabilities and infrastructures. This report also underlines increase, or the attempt to increase, the impact of attacks (especially by targeting critical infrastructure and industries). Attacks on banks by state actors have also been seen as an attempt "to avoid the negative impact of sanctions". Finally, corporations have begun using state-actor techniques for commercial gain (ENISA, 2019, pp. 116-121).

4.1. United States

The United States, who has been the leading power in many fields for the World, the advent of the new digital age has meant new challenges, as other powers have emerged, such as the EU or China. The US federal institutions have a wide array of instruments to establish cybersecurity standards. Due to the system of governance in the US, the private sector relies on state legislature while executive institutions are governed by federal regulation, in order to establish better cybersecurity standards nationwide and be able to understand how the cybersecurity policies are shaped. To improve these standards, the US uses instruments such as "hackathons, competitions, bug bounty challenges, red teaming and pen testing" as they allow for simulated attacks to play out and the government institutions are able to see the vulnerabilities exposed by the attacks. These practices have also been adopted by third states and private companies. This activity also pushes "specific cybersecurity goals", as its exposing nature proves the need for improvement in the sector.

The US has its own NIST Framework. It seeks for standardisation and improving taxonomy in the cybersecurity field. Other states, such as Israel or Japan also use this framework, which shows its clear effort for the normalisation of standards in the field.

The US started using communications as an instrument to express its own position regarding the question of cybersecurity, for this, the State Department Legal Adviser referred to a study called "The Talinn Manual", published in 2012 and updated in 2019 which further explores this question. The United States also partakes in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, endorsing the work done by the group.

Just as the European Union has done, the United States has also taken punitive action in order impose its will on attacks against cybersecurity. Extraditions, indictments and sanctions have all been used by the US for this purpose. Just like the European Union, it has developed its own cyber-related sanctions programme, implemented via executive orders (issued by the President of the United States) or statutes (passed by the Congress of the United States) which then are regulated by the Office of Foreign Assets Control.

In fact, the United States, and the European Union both share a plethora of instruments as well as they have plenty of common understandings on how cybersecurity should be regulated. Their own frameworks show their will for a long-term implementation of certain rules in the sector (Schuetze, 2020, pp. 32-41).

In 2017, President Trump signed an executive order aiming to improve the United States' cybersecurity by "engaging with engaging with international allies; ensuring the nation has strategic options to deter adversaries; and training a cybersecurity workforce" (Aegis, 2019).

4.2. China

In general, the view from China has been a positive one, as the European approach implies a multilateral take on the issue. China has also taken on the mission to learn from the European certification system and GDPR. Aligning certification standards would lead to lower costs in the long run. However, there are two looming issues: one being that Europe is ideologically closer to the United States, which could mean that conflicts between the US and China lead to issues in the relationship between the EU and China; the second one being the securitization of some IT sectors which would in turn make it more difficult for foreign companies to get certified for the European market (Lyu, 2019).

Some go as far as to claim that the Chinese approach to cybersecurity is deeply tied to the Chinese government structure, having a metaphorical stranglehold on the internet and a control of the internet and information are required to boost the legitimacy of the Chinese Communist Party in the eyes of the Chinese people. These authors also believe there is a dangerous expansion of the Chinese model in some countries (especially related to the Belt and Road Initiative), where the CIT systems are used for surveillance and control of the populace (Geller, 2018).

At the same time, China has taken a step towards technological autarky: the latest five-year plan included a target to become self-sufficient in terms of technology, as the China-US Trade War showed the CCP how dangerous it is to rely on foreign technology and know-how when producing state-of-the-art tech (namely, semiconductors). However, Chinese government officials called

for global cooperation, despite the strategic move towards self-reliance, which could mean they are preparing for the worst-case scenario and hoping for a better outcome (McGregor, 2020).

China, in fact, has been developing a cybersecurity law in the past decade. Parts of this law worked and were developed on different levels and regarded different topics. When Xi Jinping became the General Secretary of the CCP and the President of the PRC, a committee to "maintain cybersecurity" was established, which lead to drafts and subsequent amendments. In November 2016, the Cybersecurity Law of the People's Republic of China was adopted, and it came into effect on June 2017 (KPMG, 2017). However, despite all these calls for cooperation and normalisation of the cyber domain, there have been continuous reports of cyber-attacks attributed to the Chinese government or entities related to it. Most, if not all of these, have been linked to some sort of strategic or tactical move in the particular situation at the time (i.e., attacks on Indian government and banks during days where skirmishing between Chinese and Indian militaries happened, surveillance of minorities regarded as threats by the Chinese Communist Party, etc.) (Center For Strategic & International Studies, 2021).

4.3. Russia

The case of Russia is probably the most particular one among those discussed in this article, as ambiguities and contradictions can be seen here. It widely known that the questions of national security and sovereignty have been haunting the Russian Federation since it was established after the dissolution of the USSR. On top of that, Russia has inherited the "otherness" from the Soviet Union and its Cold War past in the "Western" mindset. Therefore, it has had to act decisively in terms of projecting its interests and power outwards, which further consolidated and reaffirmed the differences with its "European" neighbours and the US.

Especially relevant to the topic at hand is what has been dubbed "hybrid warfare", a broad combination of traditional warfare plus non-military measures. Some highlight that this is a part of Russian warfare culture tracing back centuries to Napoleon's invasion of Russia and the subsequent failure, part of the Russian "National Pride". This is important, as "cybersecurity" is considered as part of "information warfare", which can be deployed before any actual military intervention begins and therefore represents the most important part of the readiness for war, states Valery Gerasimov, a Russian general (Gerasimov, 2019).

For Russia, its own foreign policy in the field of cybersecurity (the Information Security Doctrine) is a response to the threat that other actors represent, especially regarding its own values and interests. This clearly shows how Russia sees itself as a victim of foreign threat and subterfuge, while the West sees this as an excuse to carry out an aggressive posture in this aspect. Officially, the Russian posture is defensive and seeking collaboration against these threats. Its focus is to establish frameworks and partnerships. However, its interpretation of cybersecurity as part of "information warfare" asks for a deeper look into its offensive cyber capabilities. The lack of clear legal frameworks acts as an incentive, as attribution is difficult and therefore hardly leads to retaliatory action, on top of being low cost (compared to traditional military or espionage operations).

It is the fact that Russia perceives itself as being threatened by other states and being vulnerable in this aspect that drives it to developing these capacities, and the fact that other states have the same vulnerability will keep motivating Russia to develop and try to lead in this field (Lilly & Cheravitch, 2020, pp. 3-20).

For Russia, all of this has been seen as an opportunity to combine its role as military superpower to engage in hybrid operations. On the other hand, regarding regulation, Russia does not see in the Chinese model "an example for the regulation of the virtual space" (Kshetri, 2016, pp. 232-233).

Figure 1 shows the evolution of the number of cybersecurity events attributed or originating from these three countries, and their upward trend, albeit at a different rate.

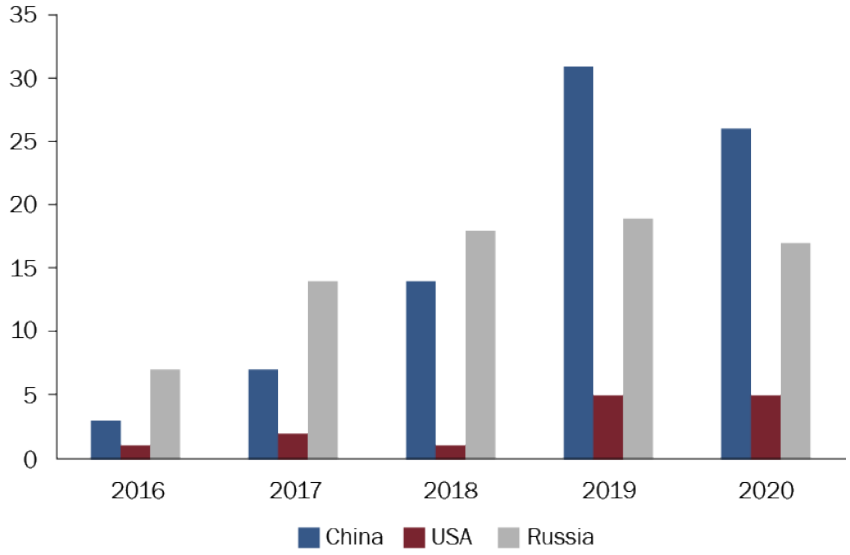

Figure 1

Number of cybersecurity events attributed to related to or originating from these states 20162020

elaborated by author, Center for Strategic & International Studies (2021).

5. Understanding these developments in the context of the European foreign policy

First, it is important to remember the fact that the European Union, relatively, a weaker player when talking about technological development in general (when compared to the USA, China or Russia). Therefore, it cannot unilaterally put pressure and force the others accept its view and regulation on these states (something it has been able to achieve regarding other topics with weaker non-EU, European states). Since its foreign policy aims to be aligned with its core values, implying that these are the values on which the norms would be based (at least, if it was up to the EU to establish those norms) and it is unable to do so unilaterally, both due to the fact that it is not a hegemonic power capable of imposing its own internal norms as international and the fact that international norms are created intersubjectively, that is, established, interpreted and played out by the international subjects (mainly, states). Therefore, it will require for the interaction of these subjects in order to establish the normal course of action in the cyber domain. The years of the "Internet Wild West" have come to an end, and different interpretations on how to legislate and what is allowed can be causes

for conflict. For the European Union to be able to make sure that its core values are part of this normal, it will have to establish itself in a position where it is able to convince the other powers about the advantages of these values and the need for such a rule based cyber-order. Different points of approach for this topic will need to be taken, and the different perspectives of the states, in some way need to pivot along on common points for the European Union to succeed.

When analysing the effects this European policy has had on the United States, there are similarities in both national policies, behaviour in the international scene and interests expressed in their communications and intentions. On top of that, a long-lasting relationship with a similar ideology must be taken into account. Both the United States and the European Union have tended to regard the "rule-based order" as the basis for international norms. This has extended into the perspective of cybersecurity, where both of them have sought similar order by creating national frameworks and tried to extend them over to other states and they have regarded international law as the rulebook for when doubts arise regarding the behaviour of states which do not align with their interests. This is understandable, as they were the ones who established the majority of these rules while "the West was best", but as their power has slowly diminished, relative to rising powers, they have left the inheritance of their great power past, which they would still like to "ride" as long as they can, exerted as a form of structural power.

For the member states of the European Union this is especially interesting, as the loss of its colonial empires has meant a major decrease in its influence worldwide, which has not been yet readjusted, and the use of normative, as opposed to civilian or military powers, colonial past, could allow it to transform some of the remnants of its colonial influence into the new "rule-based order", a concept which does not evoke images of oppression of other peoples, while still allowing for the Europeans to have an important say in international politics and "the moral high ground". This perception of the European Union as a civil power can be used to promote its own beliefs, practices, and values, moved by the fact that they are seen as legitimate, as opposed to values imposed via hard power. United States also benefits from this, but it is also able to use its hard power and ideas derived from American exceptionalism to promote its own interests. All these factors, and probably some more, contribute to a kind of synergy between the EU and the US, where despite efforts from the EU to become "strategically autonomous", it still has very deeply rooted connections with the United States, especially on the ideological level, where maintaining bourgeois democracies is fundamental to secure the democratic rule of law and institutions.

Therefore, the EU and the United States push for similar outcomes on the normative level. Of course, matters of national security and defence might still cause friction (for example, actions such as cyberespionage, especially on partner states will be major issues and the US does not have a clear record in that regard). Nonetheless, their similar and common trajectories explain why the US has not reacted by changing its foreign policy regarding cybersecurity, as many times sanctions are placed as a group for those offending the rule-based world order. Therefore, sanctions have not changed the actions of the United States in a meaningful way, as the US already was following similar policies and taking similar actions to the European Union. Similar policies and attitudes by both the EU and the US show that they are aiming in similar directions

when talking about cybersecurity norms in the international stage; however, international politics is more than that, and of course, each actor looks to maximise its gains and minimise its losses, therefore, in some fringe cases they will act independently or even have opposing interests. Nonetheless, their civil capacities and ideologies being similar, therefore they can reach common ground more easily than the other states compared in this paper. This means that it is also hard to identify who is influencing whom, as their takes on the matter are very similar and closely related. Especially when taking into consideration that an important part of the security aspect in the European Union is intertwined with NATO, cybersecurity frameworks are shared and security cooperation with the United States is very common, especially when considering that the EU is clearly the weaker partner who has more to gain in many of these aspects, it is understandable that the sanctions related to cybersecurity have not had a major impact in the way the United States behaves itself in the cyberworld in the international sphere. Ultimately, this close relationship should in fact help the EU as sharing common perspectives and being able to convince strong partners to enact measures such as sanctions makes them more effective, and both are to gain from these developments. In fact, in some respects, the EU and the US can be considered as the same bloc regarding cybersecurity norms.

The case of the People's Republic of China is a very interesting one: it is in fact the prime example of colonised nation which has slowly adopted the Westphalian system and has integrated itself into the society of states and multilateral organisations, especially since it was welcomed back into the United Nations and since it boomed economically and became part of multilateral organisations such as the WTO almost 20 years ago. It used the same rules and norms that were forced upon it by the Western world and adopted them to its own political configuration to great success. Then, with the rise to power of Xi Jinping, it came out of its slumber and began challenging some of these norms and demanded that some changed be made, as the international structures which guide the international society are overrepresenting Western ideals and it challenged the hegemonic power since the end of the Cold War, the United States of America. This change of attitude and behaviour, from Deng Xiaoping's "Observe calmly; secure our position; cope with affairs calmly; hide our capacities and bide our time; be good at maintaining a low profile; and never claim leadership." to Xi Jinping's "Chinese Dream" and "Belt and Road Initiative", the last idea presented by Deng, the idea of a non-hegemonic world. China's integration in all these multilateral structures have also been important, as it has parted ways with traditional Marxist concepts, such as promoting world revolution, for a more stable society of states, respecting internal sovereignty of each state, while demanding reciprocity in that matter. Of course, others have also adapted to China in the same way, interaction implied intersubjective creation of identities, where common ground had to be reached in order to secure a stable and normal relationship between states. This is general view is representative of what has happened in terms of cybersecurity, as the People's Republic has acquired a capacity to produce state-of-the-art technologies and it has established cybersecurity structures, on the one hand it has seen a need to create national cybersecurity frameworks, while supporting its idea of "cyber sovereignty", as to make sure that technology is always under control of the Party-

State duality. Therefore, innovative ideas and norms coming from the EU, such as the GDPR have been influential for adaption at a national level, while ideas like multilateral governance on the cyber domain and adopting international law as the basis for it have not been able to reach the core of the Chinese view. This is likely due to the fact that it would highly conflict with Chinese interests, as attacks from China have been seen to be related to the conflicts of the moment that China has been involved itself in, thus likely considered matters of national security or defence, unlikely to be transformed by normative power in such a short period of time. However, it should not be disregarded as a failure, as in the long run, higher security standards (increasing cyberattack cost), the state of international affairs in that moment and political will (ideas regarding how to avoid a cyber-arms race) could lead to normalisation of Chinese activity in the cyber domain, especially if its interests are reconfigured (for example, China itself becomes highly vulnerable to cyber threats) and tries to become a leader in promoting multilateral governance in this field (it is not hard to imagine a case similar to what the fight against the Climate Emergency has been and how it has evolved in the last 25 years). However, at the moment, the influence of the European Union has not yet been able to change the course of China towards a more rule-oriented behaviour. China seems to pay lip-service to commitments in this field while its sponsorship and permissiveness still allows for important cyberthreats to bloom. The EU is able to work as a "pivot-state" by reaching out to both China and the US, de-escalating and serving as a halfway point, helping them to work out their differences and pushing its own values into the mix.

Finally, the case of Russia is probably the most complicated one as more variables mix there. First, the legacy of Russia as the "Soviet threat" has remained well into the 21st Century. National politics, a heritage of military culture and self-perception, among others make Russia a state whose cybersecurity behaviour is hard to normalise regarding Western norms. The fact that Russia has decayed from a superpower to a regional power, but its military is still a considerable threat and probably its most important asset has led to a concentration of power and a self-projection as though Russia must seek its self-preservation mainly through force or the threat of force. Its intelligence agencies have been swift to recruit independent hackers into their forces and its military intelligence, in order to gain the edge on the other states. As its basic survival was perceived as threatened, Russia has developed its defensive capacities and it has expanded into offensive capacities as a deterrent, all of this also applying to its cybersecurity domain. However, once it acquired the offensive capacities it got involved in an arms race dynamic, where it has become a major cyberthreat in the international sphere (as weakening others makes Russia relatively stronger in comparison, it has been an advantageous development in this respect). Other dynamics with aims to isolate Russia and punish it for its policies have been found to be actually fuelling nationalist sentiments in the country thanks to a "rally-around-the-flag effect", as Western sanctions were perceived as an attack on the already punished Russian nation. On the other hand, sanctions regarding cybersecurity on Russian nationals, intelligence members and companies have not had constraining nor coercing effects, meaning that it has not been able to amplify any efforts by the EU to change the behaviour of Russia as a whole. Reports by ENISA stating that worldwide state-sponsored cyberthreats have stopped growing are

even more concerning as an increase in the scope and importance of these attacks would cause even greater disruptions on the already fragile informatic systems. Pushing for sanctions in this respect, instead of looking for a common ground, will probably further escalate the arms race and make everyone worse off, while fuelling nationalism and populism in the respective countries. All in all, a different approach should be taken to achieve a change in the Russian worldview, starting with dialogue and cooperation efforts in order to build trust, as lacking this fundamental factor, no security communities can be built.

6. Conclusions

All in all, we have seen that actions and sanctions taken by the European Union to create states with identities and interests like its own have been mixed, depending on the perspective taken to interpret these results. A superficial take on the matter would argue that the sanctions have not had the desired effect and have been detrimental for civilian populations in the target countries; nonetheless, a deeper dive and understanding of these restrictive measures shows a clearer image.

First of all, targeted sanctions allow for measures against individuals which have had some influence in the decision-taking process, or the actions taken by other states in that regard. Others argue, on the contrary, that these measures are punitive and unproductive when considering future decisions. However, the signalling purpose of sanctions interprets them as positioning the sender as clearly opposing to whatever action is being punished. Therefore, it in fact allows to shape identities of both the sender and the receiving actors – the EU as a sender portrays itself as the defender of the rule of law and non-offensive action in the cyber domain, while on the receiving end, these actors are perceived as a threat, which itself is a double-edged sword (as it can lead to arms race dynamics in the cybersecurity domain). Sanctions being the best instrument regarding opportunity-cost in this respect and with the European Union getting used to it as its strongest foreign policy tool, they have proved to not be inherently as bad as some would make believe but their effectiveness is also limited in scope, therefore requiring for a better long-term solution to these issues. Thus, our initial hypothesis stating that sanctions did not have any meaningful effects in this regard is rejected, as it has non-coercing effects in this matter.

We can also observe an attempt by these states to establish their own national cybersecurity frameworks which they aim to see adopted on an international level in order to be perceived as "leaders" in this domain. The European Union has had great success in this regard, as without being a technological superpower (especially when compared to the United States and China), it has achieved its own legislation to be studied for adaptation in the other states, without having forced it on them. Establishing its own bloc-wide policy regarding cybersecurity has allowed the European Union to follow a clear rule-based behaviour on the international scene, where its efforts are legitimated by these actions.

Each of the cases compared in this paper has its peculiarities, from the similarities in the frameworks and behaviour between the US and the EU, the interesting synergies the European framework and legislation presents itself for the People's Republic of China to the apparently great efforts needed to

reconnect, for lack of a better word, with Russia, who seems to be drifting further away from the West in this respect. The case of the US shows the most promise as cooperation has not been a major issue between these two partners. The EU could also work as a pivot between the US and China, as it tries to become strategically autonomous from the US in terms of security, cooperating in China as leverage against American hegemony. The case of Russia being the most complicated one due to the already complicated relationship the EU has with Russia regarding all other topics, where Russia has begun seeing the West as a major threat to its national security and has important concerns regarding its own national interests.

References

Aegis. (2019). White Paper on Cybersecurity Policy: Common Ground for EU-US Collaboration. AEGIS project. https://bit.ly/30Shw2G

Biersteker, T. & Portela, C. (2015). EU sanctions in context: three types. European Union Institute for Security Studies (EUISS).

Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A., ... & Gorniak, S. (2015). Definition of Cybersecurity-Gaps and overlaps in standardisation. ENISA.

Bull, H. (1995). The Anarchical society: A Study of Order in World Politics. Macmillan press.

Center For Strategic & International Studies. (2021). Significant Cyber Incidents Since 2006. https://bit.ly/3ehlu8j

Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union. (2012). Official Journal of the European Union. https://bit.ly/3piYegh

European Parliament and of the Council. (2016, 6 de julio). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://bit.ly/3pkJ1LN

ENISA. (2017). ENISA Threat Landscape Report 2016. 15 Top Cyber-Threats and Trends. European Union Agency for Network and Information Security. https://bit.ly/3eltxAI

ENISA. (2018). ENISA Threat Landscape Report 2017. 15 Top Cyber-Threats and Trends. European Union Agency for Network and Information Security. https://bit.ly/3plDqEQ

ENISA. (2019). ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. European Union Agency for Network and Information Security. https://bit.ly/32qw0au

European Commission. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. https://bit.ly/3JdbDyi

European Commission. (2020). The EU's Cybersecurity Strategy for the Digital Decade. https://bit.ly/3ySaOX3

Fernández Bermejo, D. & Martínez Atienza, G. (2018). Ciberseguridad, ciberespacio y ciberdelincuencia . Thomson Reuters Aranzadi.

Geller, E. (2018, 19 de julio). China, EU seize control of the world's cyber agenda. Politico. https://politi.co/3z72C5z

Gerasimov, V. (2019, 4 de marzo). Vektory razvitiya voennoy strategii [Vectors for the Development of Military Strategy]. Red Star. https://bit.ly/3sqYiww

Giumelli, F. (2016). The success of sanctions: lessons learned from the EU experience. Routledge.

Giumelli, F. (2013). How EU sanctions work. Chaillot papers, 129.

Giustozzi, C. (2019, 18 de abril). ENISA: The EU's Guide to the Cybergalaxy. Istituto per gli Studi di Politica Internazionale. https://bit.ly/3yRDy22

Katzenstein, P. (1996). Introduction: Alternative perspectives on national security. En P. Katzenstein (ed), The culture of national security: Norms and identity in world ¡politics (pp. 1–32). Columbia University Press.

KPMG China. (2017). Overview of China's Cybersecurity Law. KPMG. https://bit.ly/3svgANg

Kshetri, N. (2016). Quest to Cyber Superiority. Springer.

Lilly, B. & Cheravitch, J. (2020). The Past, Present, and Future of Russia's Cyber Strategy and Forces. 2020 12th International Conference on Cyber Conflict (CyCon). https://doi.org/10.23919/CyCon49761.2020.9131723

Lyu, J. (2019). Room for New Parnterships: A Chinese View on Europe's Cybersecurity. Istituto per gli Studi di Politica Internazionale. https://bit.ly/3sqoR4Z

Manners, I. (2002). Normative power Europe: a contradiction in terms? JCMS: Journal of common market studies, 40(2), 235-258. https://doi.org/10.1111/1468-5965.00353

Markopoulou, D., Papakonstantinou, V. & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

McGregor, G. (2020, 30 de octubre). China's new five-year plan has an ambitious aim: to become a self-sufficient, global tech superpower. Fortune. https://bit.ly/3EpzLKq

Portela, C. (2016a). How the EU learned to love sanctions. Connectivity wars, 36-42.

Portela, C. (2016b). Are European Union sanctions "targeted"? Cambridge Review of International Affairs, 29(3), 912-929.

Renard, T. (2018). EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. European Politics and Society, 19(3), 321-337. https://doi.org/10.1080/23745118.2018.1430720

Schuetze, J. (2020, 25 de noviembre). EU-US Cybersecurity Policy Coming Together: Recommendations for instruments to accomplish joint strategic goals. EU Institute for Security Studies. https://bit.ly/3yTpmpo

Stenhammar, F. (2004). UN smart sanctions. Political reality and international law. En D. Amneus & K. Svanberg–Torpman (eds.), Peace and security. Current challenges in international law (pp. 145–175). Studentlitteratur.

Wunderlich, C. (2020). Rogue States as Norm Entrepreneurs. Springer International Publishing.

References consulted

Manners, I. (2008). The normative ethics of the European Union. International Affairs (Royal Institute of International Affairs 1944), 84(1), 45-60.

Manners, I. (2009). The Concept of Normative Power in World Politics. Institut for Internationale Studier / Dansk Center for Internationale Studier og Menneskerettigheder.https://bit.ly/3mthuG7

Author notes

** Master's degree in International Relations, Security and Development at the Autonomous University of Barcelona (Spain). The author's research is focused on sinology, European Union external action and technology. ORCID: 0000-0001-5630-3332. E-mail: Lukas.Kondrotas@e-campus.uab.cat