CHAPTER 8

# GALACTIC COLLISION

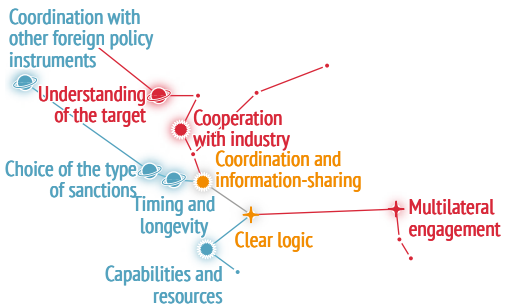
## Cyber sanctions and real-world consequences

## INTRODUCTION

Astronomers refer to colliding galaxies to describe interactions between different galaxies whose gravitational fields disturb one another. It is not a collision in the traditional sense of the word but rather a stage in the galaxies' evolution that might result in their merger. The existence and functioning of the cyber sanctions regime in parallel to the sanctions regime already put in place and the interaction with other aspects of the real world resembles such a galactic collision.

It is critical for any new cyber sanctions regime to properly identify and address how sanctions affect the cyber world, how the cyber world can favour sanctions evasion, as well as some of the challenges for the cyber world in adapting to existing sanctions. Sanctions have a number of consequences, which can be direct or indirect, as well as intended and unintended. Direct consequences can be produced by the very imposition of sanctions. For instance, an increase in the cost of fuel can be an intended consequence of an oil ban, perhaps to reduce the mobility and autonomy of military vehicles, but an increase in the costs of medicine is typically defined as an unintended consequence of sanctions. At the same time, indirect consequences can affect products/services not mentioned by sanctions. For instance, a ban on oil can contribute to a rise in petroleum costs, which indirectly causes an increase in the prices of foodstuffs and medicines. Additionally, there is the issue of the undesired but inevitable consequences of the adoption of sanctions, known in military terms as 'collateral damage': often, unfortunately, the impact which sanctions have been designed to produce comes with consequences that are indeed undesired, yet unavoidable.

**Constellation of issues in this chapter**




With this in mind, this chapter discusses aspects that should be taken into account when the cyber sanctions regime is put in place and implemented. Some of the issues addressed in this chapter are of particular importance in the context of listings – a step that the EU has so far not undertaken. But the chapter also touches upon how other sectoral, country-specific or thematic regimes can affect cooperation in the cyber domain and hinder effective responses.

# CYBER SANCTIONS AND LAW ENFORCEMENT COOPERATION

In the case of malicious cyber activities conducted from abroad, law enforcement can often only work internationally through the Mutual Legal Assistance Treaties (MLAT). As the investigative police force is typically unable to perform an end-to-end investigation, they must rely on their partners in third countries to help identify the criminal, and take any enforcement action. Such forms of cooperation usually require time in order to ensure that law enforcement agencies operate according to due process principles, including ensuring a high standard of proof for the case to be prosecuted successfully. The fact that evidence or the criminal infrastructure might be located across many jurisdictions complicates the process further. For instance, the Avalanche network used by criminal groups since 2009 for conducting malware, phishing and spam activities was dismantled only in November 2016 after more than four years of global investigative efforts that involved the support of prosecutors and investigators from 30 countries as well as the FBI, Europol and Eurojust.[1]

When there is little or no law enforcement cooperation between countries, the investigating police force's only opportunity to arrest the criminal is when he or she travels outside of their country of residence. International arrest warrants or Red Notices can be issued, but they are not always public, which can give the perpetrators a false sense of security and does not alert them to potential consequences when, for instance, they decide to travel. For example, Russian national Aleksandr Panin, accused of masterminding the SpyEye malware, was arrested while visiting the Dominican Republic.[2] In another example, Vladimir Drinkman, suspected of the theft of credit card numbers from retailer TJ Maxx, was arrested during a trip to the Netherlands.[3] Travel bans, as one type of sanction, thus have the potential of negatively affecting the ability of police forces to arrest criminals and enforce the law. This implies that when discussing possible listings, it is necessary to take into account potential adverse implications for the ongoing criminal investigations and take measures to deconflict both types of instruments. Otherwise, the effectiveness of both the cyber sanctions regime and law enforcement will be undermined.

**Sanctions regimes and criminal investigations operate on the basis of a different logic and timeframe .**

It is also important to consider how cyber sanctions might affect political relations between states and practical operational law enforcement cooperation. Due to its international nature, cybercrime can often be conducted from unfriendly or sanctioned countries, meaning that criminals are well beyond the reach of law enforcement agencies and making an investigation more difficult. In cases of non-cooperative regimes, indictments or targeted sanctions can be a last resort, but such decisions should be based on an earlier assessment of the potential negative impact on criminal investigations. Recognising that sanctions regimes and criminal investigations operate on the basis of a different logic and timeframe (i.e. political motivation and urgency in the case of sanctions regimes as compared to punitive action and a potentially longer timeframe set by due process requirements),

1 Europol, "'Avalanche' network dismantled in international cyber operation", Press Release, December 1, 2016, https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation.

2 Donna Leger Leinwand and Anna Arutunyan, "How the feds brought down a notorious hacker", *USA Today*, March 5, 2014, https://www.usatoday.com/story/news/2014/03/05/hackers-prowl-dark-web/5982023/.

3 Tom Porter, "'Don't Travel Abroad' Russia warns Hackers", *International Business Times*, July 1, 2014.

there is a need for a reconciliation between the two approaches. While some level of misalignment is unavoidable, especially when the specific crime does not rise to the level of national security significance (in contrast to many sanctions regimes), it is important to look at the whole picture of how specific listings can work in concert with law enforcement measures to punish and prevent criminal behaviour. The effectiveness of this cooperation will depend to a large extent on whether the cyber-criminal under scrutiny is acting in coordination with the government or not.

# CYBER TOOLS FOR SANCTIONS EVASION

Another interesting example concerns the interaction between the cyber world and other existing regimes, whereby cyber heists, ransomware attacks and cryptocurrencies have emerged as means to generate funds and undermine country- or sector-specific sanctions already in place.

When access to the international banking system is restricted, some states leverage cyberattacks to gain access to funding. These can involve attacks that both transfer funding through existing banks, but masking them as simple in-person withdrawals, or through cryptocurrency where the transaction may be mapped, but the receiving party is unknown. In February 2016, during an attack on the Bangladesh Central Bank, hackers leveraged and exploited the SWIFT system to transfer money to an account in the Philippines. This and other attacks were linked to North Korea through similarities in code used in otherwise attributed attacks.[4] During the WannaCry ransomware attack in 2017, over £108,000 was taken from three online bitcoin wallets that were advertised to victims for them to retrieve their encrypted data.[5] In 2018, the United States Department of Justice issued a criminal complaint charging North Korean citizen Park Jin Hyok over his involvement in both attacks and connecting him with the North Korean government's malicious cyber activities, including WannaCry.[6] In March 2019, an Expert Panel reported to the UN Security Council on a trend in the DPRK's evasion of financial sanctions 'of using cyberattacks to illegally force the transfer of funds from financial institutions and cryptocurrency exchanges.'[7]

In addition, attention among governments and the private sector is increasingly focusing on ways in which rogue actors are seeking to make use of cryptoassets in an attempt to evade sanctions. Individual, companies and other entities engaged in cryptocurrency transactions are bound by the same sanctions compliance obligations as other traditional financial activities. For instance, on 19 March 2018, US President Trump signed Executive Order EO13827 banning US persons from using any digital currencies linked to the Venezuelan government.[8] In the same month, the US Treasury's Office of Foreign Assets Control (OFAC) stated that all its existing sanctions regimes apply to all US cryptocurrency firms, including those based outside the country that supply cryptocurrency services to US persons. It added that OFAC might start to list cryptocurrency addresses pertaining to companies and individuals that are on US

**4** Emma Chanlett-Avery, Liana W. Rosen, John W. Rollins, and Catherine A. Theohary, "North Korean Cyber Capabilities: In Brief", Congressional Research Service, Washington, August 3, 2017.

**5** Samuel Gibbs, "Wannacry: hackers withdraw £108,000 of bitcoin ransom", *The Guardian*, August 3, 2017, https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom.

**6** US Department of Justice, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions", *Justice News*, September 6, 2018, https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

**7** Hugh Griffiths *et al.*, "Letter dated 21 February 2019 from the Panel of Experts established pursuant to resolution 1874 (2009) addressed to the President of the Security Council", United Nations Security Council, February 21, 2019, https://undocs.org/S/2019/171.

**8** Mark P. Sullivan, "Venezuela: Overview of U.S. Sanctions", Congressional Research Service, Washington, March 8, 2019.

sanctions blacklists.[9] But the decentralised, transnational and anonymous nature of cryptocurrency practices makes it possible for a sanctioned actor to access virtual assets from anywhere in the world without having to make use of the formal banking system. Cryptocurrency firms can engage – knowingly or otherwise – in providing services within sanctioned regimes without such transactions being easily traceable by banks' compliance departments or regulatory authorities. Equally, individuals and firms may be based in a sanctioned regime but mask their location and identity through the use of techniques such as virtual private networks (VPNs), in order to carry out transactions that may be in breach of sanctions. Furthermore, some individuals or firms acting as virtual asset peer-to-peer (P2P) exchangers are able to broker unlicensed transactions on behalf of third parties, which can open the door to money-laundering and other financial activities that might fall under sanctions.[10]

The scale of sanctions evasion based on cryptocurrency payments is not currently well-understood, however. The US Treasury's Financial Crimes Enforcement Network (FinCEN) has warned that countries such as Iran could be using cryptocurrencies to evade sanctions, suggesting that it has been involved in some $3.8 million worth of bitcoin transactions since 2013.[11] It is unclear to what degree this represents an Iranian sanctions evasion strategy and, moreover, the cited figures do not yet amount to a particularly significant sum of money. Nevertheless, some predict that the volumes of funds under question are set to continue to grow over time. Elsewhere, there is concern over efforts in sanctioned states that include Venezuela, Russia and Iran to build blockchain technology that will provide 'sanctions resistance' for their financial industries.[12] In this vein, both Russia and Iran have undergone pilot tests that make use of Hyperledger Fabric – an open source software platform for blockchain systems used by private firms – to create permissioned ledgers. In early 2018, Russia's largest bank, Sberbank, completed a $12 million corporate bond transaction, using the software to settle purchases. Despite US sanctions banning US companies from providing equity financing or debt to the bank, the software itself was not under sanctions.[13]

Compliance with sanctions is a key challenge for those dealing with the cryptoasset world. Banks and other financial institutions are less able to be sure of international sanctions compliance when relying on more traditional screening and due diligence methods. In the case of financial transactions involving traditional currencies, a given bank will typically have a detailed understanding about the transaction, including the name and location of the bank and identities of other parties involved. In contrast, cryptocurrencies are sent between anonymous actors, typically operating under pseudonyms, whereby their locations and identities are often concealed. While some details may be available, for example on public blockchains, data such as names and geographical data are not widely available. This means that there is a risk that these types of transactions may not be prevented by the financial institutions. Consequently, financial institutions are increasingly turning to technological

**Compliance with sanctions is a key challenge for those dealing with the cryptoasset world.**

9 US Department of the Treasury, "OFAC FAQs: Sanctions Compliance", 2019, https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#559.

10 David Carlisle, "Cryptocurrencies and Sanctions Compliance: A Risk That Can't Be Ignored", *Elliptic*, October 16, 2018, https://www.elliptic.co/our-thinking/cryptocurrencies-sanctions-compliance-a-risk-that-cant-be-ignored.

11 Financial Crimes Enforcement Network, "Advisory on Iran Sanctions", 2019, https://www.fincen.gov/sites/default/files/advisory/2018-10-11/Iran%20Advisory%20FINAL%2.

12 Yaya Fanusie, "Seeking Sanctions Resistance Through Blockchain Technology", *Forbes*, October 11, 2018, p. 1, https://www.forbes.com/sites/yayafanusie/2018/10/11/seeking-sanctions-resistance-through-blockchain-technology/

13 Ibid.

solutions, such as AML software, in order to review blockchain ledgers for activities occurring in sanctioned jurisdictions.[14] In February 2019, the Paris-based global standard setting organisation for countering illicit finance, the Financial Action Task Force (FATF), issued a statement that recognised the need to better mitigate risks linked to virtual asset transactions, particularly in connection with money laundering and terrorist financing.[15] Soon after, in June 2019 FATF adopted and issued an Interpretive Note to Recommendation 15 on New Technologies[16] (INR. 15) followed by the Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers.[17]

The EU has not passed specific legislation in relation to cryptocurrencies to date.[18] Regulation over cryptocurrency exchanges currently resides at the individual member state level, where there is a wide range of variation on how each country approaches the matter. Nevertheless, licences and authorisations granted by individual national regulators can 'passport' exchanges, permitting their operation across the entirety of the EU, under one licensing regime.[19] In February 2018, the president of the European Central Bank, Mario Draghi, said that work was underway to develop the Single Supervisory Mechanism in order to identify financial risks presented by virtual assets. In April 2018, the Fifth Money Laundering Directive (5MLD) was agreed by the EU, bringing cryptocurrency-fiat exchanges of currency under the EU's AML legislation and requiring KYC/CDD (Know Your Customer/Client Due Diligence) operations to be carried out on customers in line with normal reporting requirements.[20] The directive brings the EU in line with virtual assets measures introduced by the US some six years ago.[21] In early 2019, the European Banking Authority called for pan-EU rules on virtual assets, arguing that the heterogeneity of approaches to cryptocurrency regulation across the bloc could be open to exploitation.[22] In April 2019, the EU launched the International Association of Trusted Blockchain Applications (INATBA) to further efforts in this area. In a different vein, there is a risk that overregulation of crypto assets and wider digital technologies might undermine some of their potentially positive contributions to humanitarian payments executed in war zones and humanitarian crises.[23]

**14** Ibid.

**15** Financial Action Taskforce (FATF), "Public Statement – Mitigating Risks from Virtual Assets", February 22, 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

**16** Financial Action Taskforce (FATF), "Public Statement on Virtual Assets and Related Providers", June 21, 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/public-statement-virtual-assets.html.

**17** Financial Action Taskforce (FATF), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 21, 2019, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html.

**18** Robby Houben and Alexander Snyers, "Cyrptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion", European Parliament Study, July 2018.

**19** "Cryptocurrency Regulations in the EU", *Comply Advantage*, 2019, https://complyadvantage.com/knowledgebase/crypto-regulations/cryptocurrency-regulations-eu-european-union/

**20** Tom Robinson, "Inside Analysis on the Latest in Bitcoin, Ethereum & Blockchain", *Elliptic*, May 1, 2018.

**21** Ibid.

**22** Caroline Binham, "Cryptocurrencies: European Banking Authority calls for Pan-EU Rules on Crypto Assets", *Financial Times*, January 9, 2019.

**23** One Danish study argued that digital solutions can help to reduce the time required for humanitarian transactions to clear, reduce bureaucratic costs and curb corruption. See: Jeremy Nation, "Cryptocurrencies as a Vehicle for Humanitarian Aid from Denmark", *ETH News*, December 14, 2017. Their use is also being explored in contexts such as the Syrian conflict, where banking over-compliance, or 'de-risking', complicates financial payments required for the work of humanitarian organisations in the context of complex, overlapping sanctions regimes. See: Justine Walker, "The Foreign Policy Tool of Sanctions, Conflict and Ensuring Continued Access to Finance", *Journal of Financial Crime*, vol. 24, no. 3 (July 2017): pp. 480-90.

# SANCTIONS AND INCIDENT RESPONSE COOPERATION

The final example of the 'collision' is the impact of the existing sanctions regimes on cooperation in cyberspace and potentially conflicting norms. Cybersecurity incidents are rarely limited to a single state or economy, which is why international cooperation in crisis management and incident response is a key element. Since the risk factors leading to exploitation are specific to technologies, rather than state-level policies, attacks can easily spread between jurisdictions. In fact, even cyberattacks targeting a single state have had effects outside of the immediate target area. NotPetya was an atypical, destructive malware attack that in 2017 initially propagated through a malicious update for accounting software, M.E.Doc, primarily used in Ukraine. Due to the fact that many multinationals, including international shipping company Maersk, had offices in Ukraine and were required or encouraged to use the software, the attack quickly affected systems outside the physical borders of the country.[24] Stuxnet, a malware which was targeted against the Iranian nuclear programme, was quickly identified on over 200,000 computers in many countries, predominantly Iran, Indonesia and India, but also even in the US, albeit to a lesser extent.[25]

**New technologies provide ample opportunities for cyber criminals and sanctioned states to minimise the adverse effects of the sanctions imposed on them.**

In such a context, the UNGGE reports and confidence-building measures endorsed by several regional organisations also call upon states to cooperate and provide assistance when so requested by another country or organisation. To facilitate such cooperation and in order to mount an effective response during security incidents, a global community of Incident Response teams, often referred to as Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs) have come into existence.[26] In many ways, the global CSIRT community has always resembled the 'e-SOS system':[27] an international 'duty to assist' norm in which it is required to provide assistance to a victim asking for help, even when it is unknown who is threatening them.

While CSIRTs typically engage and cooperate directly with a peer CSIRT during an incident, they exchange best practices and lessons in these wider communities. Many of these networks do not have formal agreements in place between their members, but are built on a basis of trust, prior cooperation and an understanding that they derive mutual benefits from participation. During a major event, CSIRTs exchange details on the effects of an attack, and best practices on what has worked in their constituency to mitigate an attack. Other CSIRTs apply these lessons to successfully deter an ongoing attack more quickly and avoid repeating mistakes that others in the community may have made. Adversaries gain from a defender's inability to share across borders.

However, the world of the CERT/CSIRT community has been fragmented due to existing sanctions regimes which have made cooperation with countries like Iran, Russia, Sudan or

**24** Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History", *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

**25** Symantec, "W32.Stuxnet. Security Center," September 26, 2017, https://www.symantec.com/security-center/writeup/2010-071400-3123-99.

**26** These organisations focus on responding to security incidents within a particular constituency. Corporations often operate a CSIRT as part of their cybersecurity programme. Many states maintain CSIRTs with responsibility over government networks, or even operate, support, or are served by, national CSIRTs, which support citizens within the state during a cyberattack.

**27** Duncan Hollis, "An e-SOS for Cyberspace", *Harvard International Law Journal*, vol. 52, pp. 374-430.

## Limits to international cooperation: Duqu

In October 2011 Symantec published a report describing Duqu based on a study by the Budapest University of Technology and Economics.* The same month, Kaspersky Labs – a Russian-based developer of anti-malware solutions – published a blog devoted to the same malware and based on a previous investigation conducted in partnership with the Sudanese Computer Emergency Response Team. During their investigation, Kaspersky concluded that the dates of these incidents matched up with the dates that had been originally published by the Iranian authorities who back in April 2011 had identified the Stars malware.** In this case, the challenges to cooperation between different countries were twofold. First, in the wake of the Stuxnet malware, which had previously affected the same Iranian networks, there was little trust between the Iranian cyber defenders who identified the malicious code and the community of incident responders in other parts of the world. Second, Microsoft, as a US-based corporation, was subjected to a sanctions regime administered by the Office of Foreign Assets Control (OFAC) in 2011 against Iran and Sudan where the attack was first identified.*** Based on Executive Order 13059 dating from 19 August 1997, 'the exportation, re-exportation, sale, or supply, directly or indirectly, from the United States, or by a United States person, wherever located, of any goods, technology, or services to Iran' was prohibited. Conversely, the export of services from Iran to the United States is similarly prohibited.**** Even though these and a wide set of other written instructions do have exemptions, they are often hard to decipher due to their limited and complex nature. 'Services' do not necessarily imply the need for a payment, which is illustrated by the fact that general License D-1 embeds a specific exception in the Iran sanctions for communications services which are provided at no cost to the user, implying it would otherwise be covered.***** Given this uncertainty, in the Duqu case, incident responders in the United States were restricted from engaging proactively with incident responders in Iran to effectively assess the risk of the initial malware report from the country in April 2011, which otherwise might have allowed for a more effective handling of the incident.

* Microsoft, "Microsoft Security Advisory 2639658," November 3, 2011, https://docs.microsoft.com/en-us/security-updates/securityadvisories/2011/2639658.

** Aleksandr Gostev, "The Duqu Saga Continues: Enter Mr. B. Jason and TV's Dexter," *Securelist*, November 13, 2011; "Iran target of new cyberattack," *Mehrnews*, April 29, 2011.

*** Government Publishing Office, "31 CFR § 560.509 - Certain transactions related to patents, trademarks, and copyrights authorized. Iranian Transactions and Sanctions Regulations," July 1, 2015, https://www.govinfo.gov/app/details/CFR-2015-title31-vol3/CFR-2015-title31-vol3-sec560-509

**** Department of the Treasury, "Executive Order 13059 of August 19, 1997 Prohibiting Certain Transactions With Respect to Iran," August 19, 1997, https://www.treasury.gov/resource-center/sanctions/Documents/13059.pdf.

***** Department of the Treasury, "Iranian Transactions and Sanctions Regulations. 31 C.F.R. Part 560. General License D-1," February 7, 2014, https://www.treasury.gov/resource-center/sanctions/Programs/Documents/iran_gld1.pdf.

North Korea very difficult. CSIRTs and other partners in this global process are often challenged in working with sanctioned states across two main areas:

1. Trust building: Trust and technical standards that lead to a successful response in a security incident are built as a result of developing cooperative working habits prior to the incident actually unfolding. Because sanctions regimes often restrict these personal interactions, they also restrict the ability of states to set up a successful process for handling incidents, prior to their emergence.

2. Over-compliance/de-risking: as sanctions regimes are often rooted in the goal to reduce economic interaction with a state, they often inadvertently or intentionally generate the perception that all engagement is prohibited. Most attorneys involved in handling

technical cybersecurity challenges are not trained in also ensuring sanctions compliance, and incident responders, at a technical level, will often shy away from engaging with organisations or countries that are located in a sanctioned jurisdiction, regardless of the scope and depth of the actual sanctions in place. While regular engagement may be permitted under the concept of 'general licences' in specific cases of sanctions implementation, cyber 'security' may be listed under dual use or defence-related materials, which creates additional complications.

The constraints on cooperation in the case of a malware named Duqu offers a good illustration of this problem.

# CONCLUSIONS

The purpose of this chapter was to investigate how the growing complexity of the relations between existing sanctions regimes and the cyber world might affect the effectiveness of the measures. The interaction between the real and virtual world significantly increases the density of topics and issues that need to be taken into account and therefore makes decision-making more complicated from the technical, legal and operational point of view.

As this chapter has shown, new technologies provide ample opportunities for cyber criminals and sanctioned states to minimise the adverse effects of the sanctions imposed on them. Ransomware attacks or cyber heists have proven to be an effective way for targeted individuals or companies to generate funds while under the asset freeze. They are clearly measures of desperation which on one hand demonstrate that the existing sanctions do bite, while on the other hand exposing their limitations. At the same time, the rapid development of blockchain technologies exemplifies the difficulty for regulators to stay ahead of the curve and ensure that adequate legal measures are in place. From the legal perspective, designing an effective response across the physical and cyber world requires knowledge of regulations addressing technological and compliance aspects. This requires significant investments on the part of the governments, companies and other organisations willing to undertake cooperation – a critical constraint to which cyber criminals and other malicious actors are not subjected. Finally, in clearly operational terms, the rules pertaining to the physical world do not necessarily reflect the realities of the digital space. While rapid transnational cooperation is a quintessential aspect of effective response to cyberattacks and incident handling, the existing rules designed for other policy areas are simply too slow and consequently make cooperation difficult.