Loyola of Los Angeles International and Comparative Law Review

Volume 46 | Number 1 Article 2

Spring 4-6-2023

# Waking Sleeping Beauty? Exploring the Challenges of Cyber-Deterrence by Punishment

Thibault Moulin
*Catholic University of Lyon*

# Waking Sleeping Beauty? Exploring the Challenges of Cyber-Deterrence by Punishment

BY THIBAULT MOULIN*



*Dr. Thibault Moulin is an Associate Professor at the Catholic University of Lyon (France) and a Research Associate at the Federmann Cyber Security Center (Israel). I am indebted to Professor Duncan B. Hollis for his comments on an earlier draft. Email:thibault.moulin@mail.huji.ac.il.

# ABSTRACT

The application of existing rules of international law in cyberspace and lawful responses to cyberattacks have been discussed for years, but certainty is still lacking in the field. To face external cyberthreats, actors like the European Union decided to adopt restrictive measures (e.g., assets freezing and travel restrictions). Unfortunately, this system did not succeed in preventing further cyberattacks, and it has its own paradoxes. For these reasons, it may be tempting to consider the adoption of stronger collective measures. In this article, I focus on the doctrine of countermeasures, and I intend to determine whether the doctrine of countermeasures may be a sound basis to help an international organization or a coalition of like-minded states – like the European Union and its members – build a mechanism of deterrence by punishment. This system consists of convincing a potential aggressor that an attack would not be the worth the consequences, due to the harmful answer which would follow.

Keywords: deterrence; punishment; cyberthreats; international law; countermeasures; sanctions.

## I. INTRODUCTION

In 2017, the European Union found it necessary to influence the behavior of hackers in cyberspace, and to protect the integrity and security of European citizens and member states against foreign cyberthreats.[1] The so-called "Cyber Diplomacy Toolbox" was subsequently adopted. It paved the way for the adoption of common diplomatic responses – i.e., the freezing of assets and travel restrictions – against natural and legal persons responsible for certain "malicious" cyberactivities.[2] Under this regime, sanctions may be contemplated in response to "cyberattacks with a significant effect" or "attempted cyberattacks with a potentially significant effect," which constitute an external threat to the European Union or its member states.[3] A similar regime had previously been adopted by the United States, through

1. Permanent Representatives Committee 9916/17, 2017 J.O. (91) 4.
2. *Id*.
3. Council Decision (CFSP) 2019/797, art. 1, 2019 O.J. (L 129) 1, 2.

Executive Order 13694, which allowed the possibility of "blocking the property of certain persons engaging in significant malicious cyber-enabled activities." Since the adoption of this order in 2015, several individuals and entities have been subject to sanctions decided by the U.S. Department of the Treasury.[4] In contrast, the EU regime remained in a dormant state for three years. Restrictive measures were imposed by the Council of the European Union first in July 2020,[5] while others followed in October 2020.[6] These sanctions were imposed to last until May 2025.[7] Currently, eight individuals and four entities from China, Russia, and North Korea are subject to sanctions.[8] Most of the entities and individuals have links with the governments of those countries.[9] The Russians were caught after an attempt to hack the Organization for the Prohibition of Chemical Weapons (OPCW), which had been

4. Press Release, U.S. Dep't of the Treasury, Treasury Sanctions Two Individuals for Malicious Cyber-Enabled Activities (Dec. 29, 2016) (archived) [hereinafter Press Release, Cyber-Enabled Activities].

5. Council of the EU Press Release 522/20, EU Imposes the First Ever Sanctions Against Cyber-Attacks (July 30, 2020), https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/pdf [hereinafter Press Release, First Sanctions].

6. Council of the EU Press Release 707/20, Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack (Oct. 22, 2020), https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/pdf [hereinafter Press Release, Bundestag Hack].

7. Council of the EU Press Release 450/22, Cyber-Attacks: Council Extends Sanctions Regime until 18 May 2025 (May 16, 2022) [hereinafter Press Release, Extended Sanctions].

8. Council Implementing Regulation (EU) 2020/1125 of July 30, 2020, Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or its Member States, 2020 O.J (L 246) 4, 6-9; Council Implementing Regulation (EU) 2020/1536 of October 22, 2020, Implementing Regulation (EU) 2019/796 Concerning Restrictive Measures against Cyber-Attacks Threatening the Union or its Member States, 2020 O.J. L 351I, 3-4.

9. Department of Justice Press Release, U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations (Oct. 4, 2018) [hereinafter Press Release, Russian GRU Officers]. For instance, two departments from the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) – which are known as the Main Centre for Special Technologies (GTsST) and the 85th Main Centre for Special Services (GTsSS) – as well as the Head of the GTsSS (Igor Kostyukov), one military intelligence officer (Dmitry Badin), and four agents who were caught around the OPCW are currently subject to sanctions. Additionally, two Chinese citizens and the firm Huaying Haitai – who have links with APT10, a cyberespionage group sponsored by China – and the firm Chosun Expo – who have links with APT38, a criminal group sponsored by North Korea are currently subject to sanctions. It may be noted that most of these natural and legal persons were also indicted or subjected to sanctions in the United States. This was the case for the four Russian officers responsible for the attempted hacking of the OPCW.

investigating the poisoning of Sergei and Yulia Skripal.[10] They were also blamed for the Christmas attack against a Ukrainian energy provider – which resulted in a major power outage – and for the deployment of *NotPetya*.[11] It consisted in a "wiper," which means that data contained in infected computers was destroyed.[12] The attack was originally directed against Ukraine, but eventually spread internationally.[13] Additionally, Russia was involved in an attempt to destabilize the 2017 federal elections in Germany,[14] including an attack against the German Bundestag.[15] Chinese actors were behind a cyberespionage operation called *Cloud Hopper*, which stole commercial secrets from companies based within (e.g., Ericsson) and outside Europe (e.g., IBM).[16] Finally, North Korea sponsored *WannaCry*,[17] a virtual act of piracy which

10. *How the Dutch foiled Russian "cyberattack" on OPCW*, CNN (Oct. 4, 2018), https://www.bbc.com/news/world-europe-45747472 [herinafter *OPCW Cyberattack*].

11. Nicole Perlroth, Mark Scott & Sheera Frenkel, *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html; Thomas Brewster, *Ukraine Claims Hackers Caused Christmas Power Outage*, FORBES (Jan. 4, 2016), https://www.forbes.com/sites/thomasbrewster/2016/01/04/ukraine-power-out-cyber-attack/?sh=3ad14aa16fa8.

12. Financial institutions and private companies were stricken both within and outside Europe, but the consequences may have been more serious in Ukraine, as the monitoring system of the power plant at Chernobyl was broken. Maersk declared that the attack could cost the company $300 million, and Saint-Gobain, $250 million. *See also Trois cyber-incidents qui font froid dans le dos*, LES ECHOS (Feb. 7, 2018), https://www.lesechos.fr/thema/risques-2018/trois-cyber-incidents-qui-font-froid-dans-le-dos-130507 [hereinafter Trois cyber-incidents]; Andrew Griffin, '*Petya' Cyber Attack: Chernobyl's Radiation Monitoring System Hit by Worldwide Hack*, INDEPENDENT (June 27, 2017, 5:07 PM), https://www.independent.co.uk/tech/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html.

13. *Id*.

14. Kate Connolly, *Russian Hacking Attack on Bundestag Damaged Trust, Says Merkel*, THE GUARDIAN (May 13, 2020, 11:07 AM), https://www.theguardian.com/world/2020/may/13/russian-hacking-attack-on-bundestag-damaged-trust-says-merkel.

15. In Spring 2015, the German Bundestag was targeted by a malware attack, the purpose of which consisted of stealing data. The entire system was paralyzed and had to be shut down and rebooted. Agence France Presse, *'Russian Hackers' Again Target German MPs: Report*, SECURITY WEEK: CYBERCRIME (Mar. 26, 2021), https://www.securityweek.com/russian-hackers-again-target-german-mps-report; Mathias Bolinger, *Was Russia Behind 2015's Cyber Attack on the German Parliament?*, DEUTSCHE WELLE (Feb. 2, 2016), https://www.dw.com/en/was-russia-behind-2015s-cyber-attack-on-the-german-parliament/a-19017553 [https://p.dw.com/p/1HnKj].

16. Jack Stubbs, Joseph Menn & Christopher Bing, *Inside the West's failed fight against China's "Cloud Hopper" hackers*, REUTERS (June 26, 2019), https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

17. Public attribution was made by the United States and the United Kingdom. *See* Ellen Nakashima, Philip Rucker, *U.S. declares North Korea Carried out Massive WannaCry Cyberattack*, WASH. POST (December 19th, 2017), https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html; Ewan MacAskill, Alex Hern & Justin McCurry, *Facebook Action Hints at Western Retaliation Over WannaCry Attack*,

consisted of encrypting data stored on infected computers, before demanding the payment of a ransom of $300 or $600.[18]

These events seem to be part of a larger narrative and reflect the priorities of these actors: political motivations for Russia, theft of intellectual property for China, and financial gains for North Korea. Restrictive measures were described as a means of "preventing or resolving a cyberincident," or "expressing concerns and signaling them in another way."[19] If they indeed allow the European Union to express concerns and to signal them, their potential for preventing or resolving a cyberincident is disputed. In fact, attacks against Europe have dramatically increased since the beginning of the COVID-19 pandemic,[20] and concern was even raised by the United Nations and INTERPOL.[21] For instance, it was revealed that cyberincidents in Europe rose from 432 in 2019 to 756 in 2020,[22] and that there would be four times more supply chain attacks in 2021 than in 2020 — with half of those attacks attributable to Advanced Persistent Threat (APT) actors.[23] There is a strong suspicion that foreign states (including China, North Korea, Iran, and Russia) are part of the cyberattacks, even if those foreign states continue to deny any involvement in those actions.[24] In fact, "[a]ll this increased naming . . . has not obviously produced a lot of shame," and

---

THE GUARDIAN (December 12th, 2017), https://www.theguardian.com/technology/2017/dec/19/wannacry-cyberattack-us-says-it-has-evidence-north-korea-was-directly-responsible.

18. Samuel Gibbs, *WannaCry: hackers withdraw £108,000 of bitcoin ransom*, GUARDIAN (August 3rd, 2017), https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom; *See also* National Audit Office (UK), *Investigation: WannaCry cyberattack and the NHS*, (October 27th, 2017), https://www.nao.org.uk/report/investigation-wannacry-cyberattack-and-the-nhs/.

19. *Draft of the EU Council on "Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyberactivities"* 13007/17, 2017 O.J. 1, 14.

20. Nick Paton Walsh, *Serious cyberattacks in Europe doubled in the past year, new figures reveal, as criminals exploited the pandemic*, CNN (June 10, 2021), https://www.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html.

21. UNODC, *Ransomware attacks, a growing threat that needs to be countered*, UNODC (Oct. 18, 2021), https://www.unodc.org/roseap/en/2021/10/cybercrime-ransomware-attacks/story.html; INTERPOL, *INTERPOL report shows alarming rate of cyberattacks during Covid-19*, INTERPOL (Aug. 4, 2020), https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

22. Joe Tidy, *EU wants emergency team for 'nightmare' cyberattacks*, BBC (June 23, 2021), https://www.bbc.com/news/technology-57583158.

23. EUROPEAN UNION AGENCY FOR CYBERSECURITY, ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS 3 (2021), https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

24. CISCO, *What Is an Advanced Persistent Threat (APT)?*, https://www.cisco.com/c/en/us/products/security/advanced-persistent-threat.html; FIREEYE, DOUBLE DRAGON: APT41, A DUAL ESPIONAGE AND CYBER CRIME OPERATION (2019), https://content.fireeye.com/apt41/rpt-apt41; FIREEYE APT38: UNUSUAL SUSPECTS (2018), https://content.fireeye.com/apt/rpt-apt38.

there is no indication that the foreign states previously mentioned intend to stop these harmful activities.[25] In 2015 for instance, Barack Obama and Xi Jinping vowed that neither the United States nor China "will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, for commercial advantage."[26] This agreement was meant to prevent economic espionage, but failed in curbing this phenomenon.[27] It seems that "Beijing always intended to continue commercial espionage – it just intended to stop getting caught."[28] In this context, it may be tempting to consider adopting stronger measures and moving away from a regime of individual sanctions against those creating cyberthreats, towards a deterrent-based regime of cyber retaliation against states which host and sponsor hackers. Therefore, this article focuses on determining whether the doctrine of countermeasures may help an international organization or a coalition of like-minded states – like the European Union and its members – build a system of deterrence by punishment. This type of system would be consistent with the idea that foreign digital intrusions shall be subject to retaliations. Deterrence by punishment consists of convincing a potential aggressor that their attack would have harmful consequences, hence counterbalancing any expected benefit.[29] As the use of armed force may, in theory, trigger a common (military) response under Article 5 of the North Atlantic Treaty, this paper focuses on cyberattacks which are below this threshold.[30] First, I proceed with an analysis of the theory of countermeasures and deterrence, and I explain in particular the role of countermeasures in deterrence (Part II). Then, I underline the current challenges in building deterrence by punishment on the doctrine of countermeasures — i.e., the identification of internationally wrongful acts, the issue of attribution, and the (lack of) punitive effect of countermeasures (Part III). Next, I offer a few thoughts

25. Martha Finnemore & Duncan Hollis, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, 31 EUR. J. INT'L L. 969, 971 (2020).

26. Lorand Laskai & Adam Segal, *A New Old Threat*, COUNCIL ON FOREIGN RELATIONS (Dec. 16, 2018), https://www.cfr.org/report/threat-chinese-espionage.

27. *Id*.

28. *Id*.

29. Paul Cornish, *Deterrence and the Ethics of Cyber Conflict*, *in* 124 ETHICS AND POLICIES FOR CYBER OPERATIONS 1, 13 (Mariarosaria Taddeo & Ludovica Glorioso eds., 2017).

30. Libby Cathey, *How NATO is Updating its Common Defense Pact to Deal with Global Cyberattacks*, ABC NEWS (Jun. 14, 2021, 3:21 PM), https://abcnews.go.com/Politics/nato-updating-common-defense-pact-deal-global-%20cyberattacks/story?id=78271735 ; *See also* James Andrew Lewis, *Indictments, Countermeasures, and Deterrence*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Mar. 25, 2016), https://www.csis.org/analysis/indictments-countermeasures-and-deterrence.

to resolve these challenges at the EU level — i.e., a common understanding of primary rules, common attribution, and common deterrence policy (Part IV). Concluding remarks appear in the final part (Part V).

## II. THE ROLE OF COUNTERMEASURES IN DETERRENCE

Countermeasures may be described as ". . . [s]tate actions, or omissions, directed at another [s]tate that would otherwise violate an obligation owed to that [s]tate, and that are conducted by the former in order to compel or convince the latter to desist in its own internationally wrongful acts or omissions."[31] In particular, they differ from retorsions, which amount to unfriendly acts at most – i.e., acts which are wrongful not in the legal sense, but only in the political or moral sense, or are a simple discourtesy.[32] The International Law Commission (ILC) had the opportunity to identify the characteristics and conditions of countermeasures in the Draft Articles on Responsibility of States for Internationally Wrongful Acts (DARS), which were adopted in 2001 and reflect customary law.[33] As a matter of fact, countermeasures may only be adopted in response to an internationally wrongful act – i.e., a breach of international law – and are designed to put an end to such a violation.[34] Article 49(1) of the DARS indeed makes clear that "[a]n injured state may only take countermeasures against a state which is responsible for an internationally wrongful act in order to induce that state to comply with its obligations."[35] In addition, Articles 49(2) and 49(3) of the DARS underline that "[c]ountermeasures are limited to the non-performance for the time being of international obligations of the state taking the measures towards the responsible state" and they "shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question."[36] It is worth mentioning that the Draft Articles on the Responsibility of International Organizations (DARIO) are of little help here. The scope of the DARIO focuses on the "international

31. Resorting to self-defense and the plea of necessity would hardly be invocable in this situation because most cyberattacks do not amount to armed attacks and that the plea of necessity only works in desperate situations. *See* Michael N. Schmitt, *Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 700-03 (2014).

32. FRANÇOIS DELERUE CYBER OPERATIONS AND INTERNATIONAL LAW 194 (2020).

33. *See Report of the International Law Commission to the General Assembly*, 2 Y.B. INT'L L. COMM'N (pt. 2), U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part. 2).

34. *Id*.

35. *Id*.

36. *Id*.

responsibility of an international organization for an internationally wrongful act," and "the international responsibility of a state for an internationally wrongful act in connection with the conduct of an international organization."[37] Therefore, it does not provide specific guidelines about the measures that international organizations are entitled to adopt where a member state is subject to an internationally wrongful act carried out by another state.[38] In addition, relevant rules in cyberspace will certainly not be owed to an international organization like the European Union, but to states. For instance, it is a truism that if the European Union is not a state, then it cannot be a victim of a breach of sovereignty. Even if this is beyond the scope of this article, it may be mentioned that international responsibility for actions taken within the Common Foreign and Security Policy (CFSP) is also a complex question, and whether the European Union and/or member states shall be held accountable for them.[39]

Deterrence may be described as "[t]he act or process of discouraging certain behavior, particularly by fear."[40] This notion became popular in the nuclear era of the Cold War, and was conceptualized in the 1950's by authors including William Kaufmann. According to Kaufmann, a basic component of a deterrence policy consists of "the expressed intention to defend a certain interest."[41] He identified two types of deterrence – "punishment" and "denial" – and emphasized that deterrence held the capacity to "achieve the defense of the interest in question, or to inflict such a cost on the attacker that, even if he should be able to gain his end, it would not seem worth the effort."[42] In a nutshell, the point of deterrence by punishment "is to add another consideration to the attacker's calculus, . . . a function of whether the attacker believes the threat to retaliate will be carried out and the potential damage that will result if and when the retaliation occurs."[43] In contrast, deterrence by denial consists of ensuring the benefit of an action is counterbalanced by the costs incurred in carrying it out.[44] In addition, two other types of deterrence were

37. Int'l L. Comm'n, Rep. on the Work of Its Sixty-Third Session, U.N. Doc. A/66/10, at 54 (2012).

38. *Report of the International Law Commission to the General Assembly*, *supra* note 33, at 72.

39. Ramses A. Wessel, *Division of International Responsibility between the EU and Its Member States in the Area of Foreign Policy, Security and Defence Policy*, AMSTERDAM L.F., June 1, 2011, at 34.

40. *Deterrence*, BLACK'S LAW DICTIONARY (11th ed. 2019).

41. MARTIN LIBICKI, CYBERDETERRENCE & CYBERWAR, 7 (RAND Corp. eds., 2009).

42. *Id*. at 7.

43. *Id*. at 8.

44. Cornish, *supra* note 29, at 13.

conceptualized at a later point: "entanglement" and "norms." Entanglement may be described as "the existence of various interdependencies that make a successful attack simultaneously impose serious costs on the attacker as well as the victim."[45] Norms may be described as normative considerations which deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack.[46] If this article focuses on punishment, some words may be said about these other forms of deterrence (i.e., by "denial," "entanglement," and "norms"), which are often deemed to be more relevant in a cyberspace context.[47] First, it is true that states should not give up on "denial" and that better cyberdefense is likely required. It is also a truism that criminals often have a head start on law enforcement, and it is often easier to attack than to defend online; this is due to cyberattacks often taking advantage of human mistakes,[48] and businesses – particularly small ones – not being able to afford better protection.[49] They may consider that it would be more costly to secure their networks than to do the minimum required.[50] Second, "entanglement" has also not worked thus far. In fact, instead of discouraging authors of cyberattacks from acting, it has rather discouraged victims from reacting. This is particularly true *vis-à-vis* China. Despite threatening other states like Russia for similar past actions, the United States failed to adopt analogous rhetoric following the hack of Microsoft Exchange.[51] In a letter written to President Biden, Senator Mike Rogers highlighted that "[a] failure in this situation to punish the People's Republic of China in a manner comparable to our response to Russian hostilities creates an unacceptable double standard in this era of great power competition," and implored him "to impose significant sanctions."[52] The North Atlantic Treaty

45. Joseph Nye, *Deterrence and Dissuasion in Cyberspace*, 41 Int'l Sec. 44, 58 (2017).

46. *Id*. at 60.

47. *Id*. at 45.

48. Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773, 789 (2012); Sue Poremba, *Are Businesses Underinvesting in Cybersecurity?* CYBERSECURITY DIVE (Feb. 16, 2021), https://www.cybersecuritydive.com/news/security-budgets-enterprise-CISO/595036/.

49. Zach West, *Young Fella, If You're Looking for Trouble I'll Accommodate You – Deputizing Private Companies for the Use of Hackback*, 63 SYRACUSE L. REV. 119, 129 (2012)

50. Talbot Jensen, *supra* note 48, at 790.

51. Letter from Mike Rogers, Comm. On Armed Services, to Joseph R. Biden (Jul. 21, 2021), https://republicans-armedservices.house.gov/sites/republicans.armedservices.house.gov/files/21-07-21%20RM%20Rogers%20letter%20to%20POTUS%20on%20response%20to%20PRC%20cyber%20actions.pdf.

52. *Id*.

Organization (NATO),[53] the European Union,[54] and the United Kingdom[55] protested, but did not adopt further sanctions. Reporters from the New York Times noticed that "[t]he coalition of nations, which included the European Union and for the first time all NATO members, stopped short of punishing China." This highlights the challenges of confronting a nation with deep economic ties around the world. "Europe has lucrative trade agreements with China and has been reluctant to publicly criticize the country in the past."[56] Hence, political considerations also carry considerable weight in this situation, and the United States and the European Union are in fact China's main trading partners.[57] It is arguable, though, that none of these partners – including Beijing – has an interest in ending commercial relations. In fact, even if China depends increasingly on domestic consumption,[58] part of exports in China's GDP still amounted to 18.5 percent in 2019.[59] Third, the normative and reputational aspect of deterrence has not succeeded either. As explained above, foreign nations like China, Russia, or North Korea were not prevented from launching cyberattacks even if they regularly face hacking scandals. In fact, deterrence by punishment may have merits in cyberspace, as failure to react leaves the door open to impunity and further violations, which diplomatic tools have been unable to prevent thus far. Andrew Guzman's position *vis-à-vis* retaliation is particularly interesting in that respect:

> [a] retaliating state is communicating to the violating state and, potentially, to other states, that it will react when its legal rights are compromised. If successful, the act of retaliating will

53. North Atlantic Treaty Organization Press Release IP 21/210, Statement by the North Atlantic Council (July 19, 2021). [hereinafter Statement] (statement by North Atlantic Council).

54. European Union Council Press Release IP/21/615, China: Declaration by the High Representative on Behalf of the European Union Urging Chinese Authorities to Take Action Against Malicious Cyberactivities Undertaken From its Territory (July 19, 2021). [hereinafter China: Declaration] (declaration of High Representative).

55. UK and Allies Hold Chinese State R*esponsible for a Pervasive Pattern of Hacking*, NATIONAL CYBER SECURITY CENTRE (July 19, 2021), https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking [hereinafter UK and Allies].

56. Zolan Kanno-Youngs & David E. Sanger, *U.S. Accuses China of Hacking Microsoft*, N.Y. TIMES (July 19, 2021), https://www.nytimes.com/2021/07/19/us/politics/microsoft-hacking-china-biden.html?smid=url-share.

57. *Id*.

58. Yenn Nee Lee, *McKinsey Research Finds the World Becoming More Exposed to China-but Not the Reverse*, CNBC (July 15, 2019), https://www.cnbc.com/2019/07/15/mckinsey-world-has-become-more-exposed-to-china-but-not-the-reverse.html.

59. *China: Exports, percent of GDP*, THE GLOBAL ECONOMY.COM (2021), https://www.theglobaleconomy.com/china/exports (last visited Jan. 5, 2022).

> enhance the retaliating state's reputation as one that punishes a violator. The impact of such a reputation, of course, is to increase the expected cost of violating an agreement with that state. By retaliating, the state hopes to generate its own reputational capital that will induce its partners to comply more with their legal obligations. In effect, a reputation as a state that retaliates against violators creates an additional enforcement tool.[60]

A failure to take punitive actions, however, sends a contrary signal: a reputation of one that does not punish violators. This means there is little cost for hackers, which opens the door to further attacks. And indeed, it seems that states like China, Russia, and North Korea have already launched a series of cyberattacks below the threshold of the use of force and that victims' reactions did not prevent them from striking again. For instance, Ben Buchanan suggested that "states should recognize the value that a firm response can provide, particularly when that response does not risk military or intelligence escalation," as "[t]o do otherwise is to invite trouble. A state with no red lines is ripe for intrusion, and a state fearing serious intrusions is most at risk for the cybersecurity dilemma."[61] It may also be observed that "demystifying norms of when states may use counter cyberoperations will clarify the expectations of perpetrator states as to when victim states will respond to CNAs [computer network attacks] with counter CNAs" –[62] and that, "[w]hen we do choose to act, we need to model the rules we want others to follow since our actions set precedents."[63]

As surprising as it may seem, the connection between countermeasures – i.e., responses to an internationally wrongful act – and

60. ANDREW GUZMAN, HOW INTERNATIONAL LAW WORKS: A RATIONAL CHOICE THEORY 46-7 (2010). *See also* JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW 102-03, 225 (2005).

61. BEN BUCHANAN, THE CYBERSECURITY DILEMMA: HACKING, TRUST AND FEAR BETWEEN NATIONS 46 (2016).

62. Manny Halberstam previously noted that "[t]he prevailing legal ambiguity about how states can lawfully respond to CNAs gives rise to international normative uncertainty about how states ought to respond to CNAs. This, in turn, creates a practical unpredictability as to how states will actually respond to CNAs. Because deterrence is predicated on predictability of an undesired response, prospective perpetrator states will be less deterred from striking other states with CNAs if there is no predictable response that victim states will take." *See* Manny Halberstam, *Hacking Back: Reevaluating the Legality of Retaliatory Cyberattacks,* 46 GEO WASH. INT'L L. Rev. 199, 206-07 (2013). For more general observations about the deterrent effect of normative clarification, *see also* Catherine Lotrionte, *A Better Defense: Examining the United States' New Norms-Based Approach to Cyber Deterrence*, 14 GEO J. INT'L AFF. 75 (2013).

63. *Intel Chiefs Testify on Russian Hack* (CNN television broadcast Jan. 5, 2017).

dissuasion, are not expressly mentioned in the DARS.[64] Yet, this issue was discussed during the *travaux préparatoires*, as several states agreed that fear of countermeasures may prevent breaches of international law in the first case but nevertheless found it necessary to prevent abuses.[65] In his fourth report, Special Rapporteur Willem Riphagen underlined that "the fear of reprisals is one of the main reasons for voluntary performance of international obligations."[66] Years later, Denmark (on behalf of the Nordic countries) agreed that "[i]n particular cases the risk of countermeasures may actually be the only effective deterrent to the commission of internationally wrongful acts."[67] In fact, it was described as "a reflection of the imperfect structure of present-day international society, which has not (yet) succeeded in establishing an effective centralized system of law enforcement" – and was actually "firmly founded in customary international law."[68] Yet, an appeal to punishment was disapproved by various states, even where it was conflated to a financial aspect (i.e., reparation and the payment of punitive damages).[69] Further, Denmark (on behalf of the Nordic countries) "wish[ed] to underline that countermeasures should not be resorted to as a punitive function, but should be seen as a remedy designed to induce the wrongdoing state to resume the path of lawfulness."[70] As they also said: "in other words, punitive actions are outlawed."[71] France "d[id] not believe that an internationally wrongful act should expose the wrongdoing state to punitive legal consequences," as "such a function ha[d] hitherto been unknown in the law of international responsibility, which has emphasized making reparation and providing compensation."[72] Punitive action was also rejected by Mexico.[73] The Czech Republic and

64. *Report of the International Law Commission to the General Assembly*, *supra* note 33, at 22.

65. *Id*.

66. Willem Riphagen (Special Rapporteur), Int'l Law Comm'n, Fourth Rep. on the Content, Forms & Degrees of Int'l Resp. (Part 2 of the Draft Articles), U.N. Doc. A/CN.4/366, at 18 (1983), [hereinafter Riphagen Fourth Report].

67. Int'l Law Comm'n, Comments & Observations Received by Governments, 50th Sess., U.N. Doc. A/CN.4/488, at 152 (1998), [hereinafter Comments & Observations A/CN.4/488].

68. *Id.*

69. For the opinions expressed by France, the United Kingdom, Austria, the United States and Korea, *see* Int'l Law Comm'n, Comments & Observations Received from Governments, 53d Sess., U.N. Doc. A/CN.4/515, at 64-72 (2001), [hereinafter Comments & Observations A/CN.4/515]

70. Comments & Observations A/CN.4/488, *supra* note 67.

71. Comments & Observations A/CN.4/515, *supra* note 69 at 84.

72. France initially disagreed with a discussion on countermeasures, considering that '[w]hile it is true that countermeasures have a reparations dimension, they also have a protective dimension and a punitive dimension.' *See* Comments & Observations A/CN.4/488, *supra* note 67, at 152.

73. Comments & Observations A/CN.4/515, *supra* note 69 at 83.

Jordan, who praised punishment due to its dissuasive value, were quite isolated.[74]

## III. CURRENT CHALLENGES IN BUILDING DETERRENCE BY PUNISHMENT ON THE DOCTRINE OF COUNTERMEASURES

In this part, I explain that three main challenges exist where the implementation of deterrence by punishment on the basis of the doctrine of countermeasures is contemplated: the identification of internationally wrongful acts (3A), the issue of attribution (3B), and the lack of a punitive effect of countermeasures (3C).

### *A. The Identification of Internationally Wrongful Acts*

Countermeasures consist in otherwise unlawful measures, which are adopted in reaction to illegality – i.e., a breach of international law. It therefore means that positive rules must be clearly identified in the first instance. If not, it is the state that claimed the right to respond that runs the risk of being accused of breaching international law. However, it is a truism that the identification of rules – or the way they shall apply – has proved to be particularly difficult in a cyberspace context. Some form of consensus exists on the use of force and armed attacks – as most states seem to agree that a cyberattack which results in injury, death, or physical damage is contrary to international law – but this is not the case for other rules.[75] The principle of non-intervention is hardly applicable in its

74. Prague argued that "[i]ntroducing the concept of punitive damages in the draft articles would make it possible to attribute to the regime for 'crimes' a valuable a priori deterrent function, and the problems involved . . . ." *See* Comments & Observations A/CN.4/488, *supra* note 67, at 150. Amman also made a declaration regarding 'serious breaches' of 'an obligation arising under a peremptory norm of general international law', which call for a collective reaction: "[t]he collective reaction of the international community of States to a serious breach of the obligations owed to it and essential for the protection of its fundamental interests [is] an important deterrent. *See* U.N. GAOR, 52d Sess., 18th mtg. at 3, U.N. Doc. A/C.6/55/SR.18 (Oct. 27, 2000), [hereinafter UNGA].

75. Kersti Kaljulaid, Estonian President, Estonia's Positions on the Applicability of International Law in Cyberspace at 4 (May 29, 2019), https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Remarks+by+the+President+of+the+Republic+of+Estonia+at+the+Opening+of+CyCon+2019.pdf.

French Ministère des Armées, International Law Applied to Operations in Cyberspace, at 7 (Oct 2019), https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjrrN-a3ov6AhWeLkQIHdyCApsQFnoECAkQAQ&url=https%3A%2F%2Fdocuments.unoda.org%2Fwp-content%2Fuploads%2F2021%2F12%2FFrench-position-on-international-law-applied-to-cyberspace.pdf&usg=AOvVaw3LFmiBylbNd8sJUHqjG2AK.

Fin. Gov't, International Law and Cyberspace –Finland's National Positions, at 6 (2002), https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf%20/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859.

current form, whereas disagreement culminates – including on the European sphere – regarding sovereignty. If people had died when *WannaCry* hit the NHS (e.g., due to interruptions in emergency medical procedures), when *NotPetya* hit Chernobyl power plant (e.g., due to incidental radioactive fallout), or over the 2015 Christmas attacks against electricity providers (e.g., due to the cold weather), then a breach of the prohibition to use force may have occurred (provided that, in this situation, an armed conflict did not already exist between Ukraine and Russia). However, the breaches only resulted in economic and data loss.[76] Even if some of these attacks caused serious financial damage or interfered with elections, they can hardly be described in terms of prohibited interventions. In order to qualify as prohibited interventions, methods of coercion must be used within the *domaine réservé* of another state (i.e., the areas of State activity that are internal or domestic affairs of a state and are therefore within its domestic jurisdiction or competence).[77] However, few areas – including electoral processes or main economic orientations – are now totally isolated from international law, and states are not compelled to do or refrain from doing something in these situations.[78] Depending on the country under attack, the same pattern of behavior may or may not be described as a breach of sovereignty. The reading of this principle may be more (France,[79]

Neth. Gov't, Appendix –International Law in Cyberspace, at 3-4 (2019), https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/Appendix_+International+Law+in+Cyberspace+(Statement+by+the+Netherlands).pdf.

Jeremy Wright, the UK Attorney General, Cyber and International Law in the 21st Century (May 23, 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

Cuban Ministry of Foreign Affairs, *71 UNGA*: *Cuba at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, REPRESENTACIONES DIPLOMÀTICAS DE CUBA EN EL EXTERIOR (June 23, 2017), http://misiones.cubaminrex.cu/en/un/statements/71-unga-cuba-final-session-group-governmental-experts-developments-field-information.

76. *Id*.

77. Katia Ziegler, *Domaine Réservé* [*Reserved Domain*], MPEPIL, para.1. (April 2013), https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1398.

78. Thibault Moulin, *Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward*, 25(3) CONFLICT & SECURITY L. 423 (July 31, 2020), *available at* https://doi.org/10.1093/jcsl/kraa011.

79. French Ministère des Armées, *supra* note 75, at 7.

Finland[80]) or less broad (Germany,[81] the Czech Republic[82]), whereas some states like the United Kingdom consider it irrelevant in cyberspace.[83] France, Finland, or Germany would likely describe *any* attack on the healthcare system as a breach of sovereignty, whereas an interruption or grave consequences for public health would be required by the Czech Republic. France, Finland, or the Czech Republic would describe any situations where major companies suffer grave economic loss as sovereignty breaches, whereas a higher threshold would be required by Germany, where the targeted company shall be of "special public interest."[84] However, due to the exercise of inherently governmental functions or critical infrastructures that would be interfered with, an attack on the Czech, French, Finnish, or German Parliament would likely qualify as such. In contrast, the attempt at hacking the OPCW clearly constituted an abuse of diplomatic immunity.[85]

Economic sanctions – which were adopted by the European Union and the United States – are lawful, albeit unfriendly measures. In the *Nicaragua* case, the ICJ was "unable to regard such action on the economic plane . . . as a breach of the customary-law principle of non-intervention."[86] The UN Secretary-General also said that "[t]here is no clear consensus in international law as to when coercive measures are improper, despite relevant treaties, declarations and resolutions adopted in international organizations which try to develop norms limiting the use of such measures."[87] For this reason, the existence of an internationally

80. Fin. Gov't, *supra* note 75, at 2.

81. German Federal Government, *On the Application of International Law in Cyberspace* (March 5, 2021) at 3-4, *available at* https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

82. Richard Kadlčák, Second Substantive Session of the Open-ended Working Grp. on Dev.s in the Field of Info. and Telecomm.s in the Context of Int'l Sec., Statement Submitted by the Czech Republic Special Envoy for Cyberspace Director of Cybersecurity Department Richard Kadlčák (Feb. 11, 2020), https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.

83. Jeremy Wright, *supra* note 75; *See also* Roy Schöndorf, Isr. Deputy Att'y Gen., Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations, Keynote Speech at the Stockton Center for International Law, U.S. Naval War College's event on "Disruptive Technologies and International Law" (Dec. 8, 2020), *in* 97 I.L.S., 2021, at 315, 405.

84. German Federal Government, *supra* note 81, at 4.

85. Vienna Convention on Diplomatic Relations, art. 41(1), Apr. 18, 1961, 23 U.ST. 3327, 500 U.N.T.S 95 [hereinafter *Vienna Convention*].

86. Nicar. v. U.S., 1986 I.C.J. at para. 245.

87. U.N. Secretary-General, *Economic Measures as a Means of Political and Economic Coercion Against Developing Countries*, para. 2(a), U.N. Doc. A/48/535 (Oct. 25, 1993); [hereinafter *Economic Measures*]; *see also* Barry Carter, *Economic Sanctions*, *in* MAX PLANCK

wrongful act is not a preliminary step to deploy the restrictive measures. Doubt surrounding the (un)lawfulness of cyberattacks also justifies the adoption of restrictive measures. It is worth underlining that the main benefit of the regime defined by the European Union seems to be flexibility. In fact, sanctions may be adopted in response to "cyberattacks," which cover various types of behaviors: access to information systems, information system interference, data interference, or data interception. These cyberattacks must also "constitut[e] a threat to member states,"[88] which means that they affect systems related to "critical infrastructure,"[89] "services necessary for the maintenance of essential social and/or economic activities,"[90] "critical state functions,"[91] "the storage or processing of classified information,"[92] or "government emergency response teams."[93]

The other side of the coin, however, is that the EU regime also sounds like an admission of powerlessness to bring more clarity on the application of international law to the so-called "malicious" activities.[94] While authors often consider that sanctions send normative signals and may reinforce emerging norms,[95] these signals are – in the present case – ambiguous at best. The European Union expressly affirmed that they "might constitute wrongful acts under international law," and considered that cyber-sanctions could be used "to prevent or respond to a malicious cyberactivity, including in cases of malicious cyberactivities that do not rise to the level of internationally wrongful acts but are considered unfriendly acts."[96] However, the concrete implementation of sanctions did not allow for a better understanding of what is "wrongful" and what is "unfriendly." If those decisions came with a description of the impugned behaviors, there was no indication regarding their liceity.[97] This may be problematic, as accusations – i.e., signaling that a given

ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW para. 30 (2001), https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1521?prd=OPIL#.ZAvDUMCMT8I.mailto.

88. Council Decision (CFSP), *supra* note 3, at Art. 1(4). Attacks on foreign firms like IBM were nevertheless deemed a satisfactory ground to adopt sanctions.

89. *Id.* at art. 1(4)(a).

90. *Id.* at art. 1(4)(b).

91. *Id.* at art. 1(4)(c).

92. *Id.* at art. 1(4)(d).

93. *Id.* at art. 1(4)(e).

94. Council Decision (CFSP), *supra* note 3, at Art. 1(4).

95. GUARDIAN OF THE GALAXY: EU SYBER SANCTIONS AND NORMS IN CYBERSPACE 5 (Patryk Pawlak & Thomas Biersteker eds., 2019), https://www.jstor.org/stable/resrep21136.9.

96. EU Council, *supra* note 19, at 5.

97. DELERUE, *supra* note 32, at 431.

behavior is bad – might have two positive effects.[98] First, they "may be constitutive of new norms and law, or new interpretations of their meanings."[99] Second, they "play a key role in constructing new norms from scratch," as they "lay out the contours" of undesirable behavior.[100] This "proposal" may subsequently gain acceptance (or not). I will have the opportunity to discuss attribution a bit further, but it may be noted that protest – i.e., "a formal objection by subjects of international law against conduct or a claim purported to be contrary to or unfounded in international law" – may have similar benefits.[101] The European Union missed the step here. In fact, the European Union has advocated for the application of international law in cyberspace for a long time, and endorsed the voluntary non-binding norms, rules and principles of responsible state behavior, articulated by the United Nations Group of Governmental Experts (UNGGE) as well.[102] However – and this happened before at the last Open-ended Working Group (OEWG) – no clear interpretation of the existing law was given.[103]

### *B. The Issue of Attribution*

It may be underlined that, according to Article 2 of the DARS, "[t]here is an internationally wrongful act of a state when conduct consisting of an action or omission: (a) is attributable to the state under international law; and (b) that act constitutes a breach of an international obligation of the state."[104] Yet – in the European Union for instance – it has been decided that a clear-cut distinction between attribution and restrictive measures must be drawn.[105] In the opinion of the European Union, restrictive measures do not amount to attribution to a state or non-

98. Finnemore & Hollis, *supra* note 25, at 976.

99. *Id.* at 981.

100. *Id.* at 982.

101. Christophe Eick, Protest, in MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW paras. 1, 13-14 (2006).

102. *Joint Communication to the European Parliament and the Council on Resilience, Deterrence, and Defence: Building Strong Cybersecurity for the EU*, at 18, JOIN (2017) 450 final (Sept. 13, 2017) [hereinafter *Joint Communication*].

103. Joint Comments from the EU and its Member States on the Initial "pre-draft" Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunication in the Context of International Security, 3-5 (2020), https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf [hereinafter OEWG Joint Comments].

104. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*, in Report of the International Law Commission on the Work of Its Fifty-third Session, UN GAOR, 56th Sess., Supp. No. 10, at 39, UN Doc. A/56/10 (2001) [hereinafter DARS with Commentaries].

105. GUARDIAN OF THE GALAXY, supra note 95, at 52-53, 67.

state actor.[106] Attribution is indeed described as a "sovereign political decision," which is "based on all-source intelligence," "taken on a case-by-case basis," and "established in accordance with international law of state responsibility."[107] However, the alleged distinction between restrictive measures and attribution may be overstated, and this is especially true in light of the principle of due diligence.[108] According to the first approach to due diligence, which flows from the *Corfu Channel* case, it is "every state's obligation not to knowingly allow its territory to be used for acts contrary to the rights of other states."[109] This means that states shall not tolerate the perpetration of wrongful acts from their own territory.[110] A problem with the application of this conception is that, as highlighted above, what is wrongful (or not) has not yet been clearly defined. However, an alternative reading of this principle exists, where due diligence is also about transboundary harm. According to a second approach, which flows from the *Trail Smelter* case, "[a] state owes at all times a duty to protect other states against injurious acts by individuals from within its jurisdiction."[111] According to a third and emerging approach, which reconciles both conceptions, states would be obliged to prevent both wrongful acts and transboundary harm.[112] This means that states shall not tolerate activities that result in damaging consequences abroad (i.e., the kind of cyberattacks with a significant effect that are usually subject to EU sanctions). In fact, when restrictive measures are decided – especially in light of the supporting pieces of information they provide – a foreign state can no longer ignore that hackers are acting from within one's own territory, and the position is even more untenable where a state's own services are targeted.[113] If it fails to react, then due diligence may have been breached. As Jan Messerschmidt put it, "[w]hen a state

106. *Id*.

107. Council Decision (CFSP), *supra* note 3, at 13.

108. THIBAULT MOULIN, LE CYBER-ESPIONNAGE EN DROIT INTERNATIONAL, at 97 (2021); THIBAULT MOULIN, CYBER-ESPIONAGE IN INTERNATIONAL LAW: SILENCE SPEAKS, at 98-99 (2023).

109. Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 22 (Apr. 9).

110. TALITA DIAS & ANTONIO COCO, CYBER DUE DILIGENCE IN INTERNATIONAL LAW, OXFORD INST. FOR ETHICS, L. AND ARMED CONFLICT at 130-33 (2021), https://www.elac.ox.ac.uk/wp-content/uploads/2022/03/finalreport-bsg-elac-cyberduediligence ininternationallawpdf.pdf ("Although most acts contrary to the rights of other states are internationally wrongful acts, the overlap is not complete.").

111. Trail Smelter arbitral award: Trail Smelter Case (U.S. v Can.), Arbitral Award, 1941 3 R.I.A.A. 1911, 1963 (Mar. 11).

112. DIAS & COCO, *supra* note 110, at 124.

113. Yuliya Miadzvetskaya, *Cyber Sanctions: Towards a European Union Cyber Intelligence Service?*, COLLEGE EUR. At 2 (Feb. 2021), https://www.coleurope.eu/sites/default/files/research-paper/miadzvetskaya_cepob_1-2021_final_0.pdf.

fails to prevent transboundary cyberharm, its breach of that obligation entitles offended states to respond through the use of proportionate countermeasures."[114]

A state may well decide to reject the "accusations" made against its nationals,[115] but it would lack credibility. It is indeed hard to argue that restrictive measures are adopted in a discretionary fashion (i.e., lightly and without solid supporting evidence). In fact, the institutions of the European Union, as well as national authorities which implement EU law, must comply with the Charter of Fundamental Rights (CFR).[116] In cases where the Charter does not apply, the protection of fundamental rights is guaranteed under the constitutions and constitutional traditions of EU countries and international conventions they have ratified.[117] Both the CFR and the ECHR protect the right to a fair trial.[118] The European Union reaffirmed that restrictive measures respect fundamental rights, especially due process and the right to an effective remedy.[119] Indeed, on previous occasions, the ECJ had the opportunity to set requirements on proof, including the right for a targeted person to "be placed in a position in which he can effectively make known his view of the evidence adduced."[120] Disrespect for those guarantees may be sanctioned,[121] as well as state refusal to transmit evidence to the ECJ.[122] Of course, according to the DARS, state responsibility is only triggered for the conduct of organs (Article 4), persons or entities exercising elements of governmental authority (Article 5), organs placed at the disposal of a state by another state (Article 6), and persons who are "acting on the instructions of, or under the direction or control of, that state in carrying out the conduct"

114. Jan E. Messerschmidt, *Hackback: Permitting Retaliatory Hacking by Non-State Actors as Proportionate Countermeasures to Transboundary Cyberharm*, 52 COLUM. J. TRANSNAT'L L. 275, 313 (2013).

115. Anton Moiseienko & Saskia Hufnagel, *Targeted Sanctions, Crimes and State Sovereignty*, 6 NEW J. EUR. CRIM. L. 351, 364 (2015) (explaining that even though sanctions are not necessarily of a "criminal" nature, they must comply with these standards).

116. When Does the Charter Apply?, EUR. COMM'N, https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu/eu-charter-fundamental-rights/when-does-charter-apply_en (last visited Oct. 2, 2022).

117. *Id*.

118. *Sanctions Guidelines – Update*, ¶¶ 9-10, 15, SEC (2017) 15598/17 (Dec. 8, 2017).

119. *Id*.

120. Case T-49/07, Fahas v. Comm'n, 2010 E.C.R. II-5555; *See also* Case C-348/12, Council v. Naft, ECLI:EU:C:2013:776, ¶¶ 66-71 (Nov. 28, 2013); Case T-228/02, Organisation des Modjahedines du Peuple d'Iran v. Council, 2006 E.C.R. II-4665; Iain Cameron, *EU Sanctions and Defence Rights*, 6 NEW J. EUR. CRIM. L. 335 (2015).

121. Case T-85/09, Kadi v. Comm'n, 2010 E.C.R. II-5177, ¶ 171-176 (30 Sept. 2010).

122. Case T-284/08, People's Mojahedin Org. of Iran v. Council, ECLI:EU:T:2008:550, ¶ 73 (Dec. 4, 2008).

(Article 8).[123] It means, *a contrario*, that state responsibility is excluded where the act had no connection with the official function and was, in reality, only the act of a private individual.[124] A government may well declare that an agent went rogue and decided to launch cyberattacks in their free time. However, in this situation, a lack of reaction against the hacker would seem suspicious. For instance, following the hacking of the U.S. Office of Personnel Management, China decided to identify and arrest several Chinese citizens rather than admitting responsibility. China claimed that the citizens were the real culprits, even though the charges were "regarded as suspect."[125] As explained above, though, "accusations" made by the European Union against a foreign national would be made in accordance with due process rights, which makes arbitrariness unlikely. In addition, the DARS underlines that "a state may be responsible for the effects of the conduct of private parties, if it failed to take necessary measures to prevent those effects,"[126] and due diligence is relevant in cyberspace.

### *C. The Lack of a Punitive Effect of Countermeasures*

The lack of clarity between lawful and unlawful behaviors is a major problem when responses to cyberattacks are contemplated. This issue was underlined by U.S. Deputy Michelle Markoff following the failure of the third UNGGE in 2017:

> [a] report that . . . omits a discussion of the lawful options states have to respond to malicious cyberactivity they face would not only fail to deter states from potentially destabilizing activity, but also fail to send a stabilizing message to the broader community of States that their responses to such malicious cyberactivity are constrained by international law.[127]

Yet, where a state was subject to a cyberattack and considers striking back, another controversy may be presented: it is disputed

123. DARS with Commentaries, *supra* note 104, at 39.

124. Estate of Caire (Fr.) v. United Mexican States, 5 R.I.A.A. 516, 531 (June 7, 1929).

125. Finnermore & Hollis, *supra* note 25, at 25.

126. DARS with Commentaries, *supra* note 104, at 39.

127. Michele G. Markoff, *Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.S. DEP'T OF STATE (June 23, 2017), https://2017-2021.state.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/index.html.

whether the doctrine of countermeasures allows retaliations and punitive actions.[128] In fact, state doctrine often mentions that countermeasures shall stop as soon as the unlawful behavior have stopped *per se*. For instance, France underlined that they "form part of a peaceful response, their sole purpose being to end the initial violation,"[129] and Finland, that "[c]ountermeasures may only be taken with the purpose of ensuring compliance, not for retaliation."[130] Australia and the United States had a similar position,[131] and this view was shared by the experts who drafted Tallinn Manual 2.0.[132] They indeed underlined that, under the doctrine of countermeasures, "[p]unishment and retaliation are impermissible purposes."[133] It may be noted that, prior to the adoption of countermeasures, the responsible state was to be called upon to fulfill its obligation and be informed of the injured state's decision to resort to them,[134] except if there was an urgent need to preserve some rights.[135] Both of these conditions are motivated by the need to prevent further escalation.[136] However, these requirements do not always match well with the particularities of cyberthreats.[137] Even if states develop greater capacity for attribution and the time between discovery and attribution gets shorter in the future, it is not rare that a cyberattack has already ceased by the time victim states can identify who was responsible for it. For instance, the hacking of the German Bundestag allegedly occurred in May 2015, but it was not until May 2016 that the Federal Office for the Protection of the Constitution put the blame on Russia.[138] The existence of *Petya* and *NotPetya* was revealed in May 2016 and June 2017, respectively, but attribution was officially made in February 2018.[139]

128. DELERUE *supra* note 32, at 441.

129. French Ministère des Armées, *supra* note 75, at 4.

130. Fin. Gov't, *supra* note 75, at 5.

131. Brian J. Egan, *International Law and Stability in Cyberspace*, 35 Berkeley J. INT'L L. 169, 178 (2017).

132. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 16 (Michael N. Schmitt ed., 2d ed. 2017).

133. *Id*. at 116.

134. DARS with Commentaries, *supra* note 104, at 135.

135. *Id*.

136. TALLINN, *supra* note 132, at 117.

137. Kenneth Geers, The Challenge of Cyber Attack Deterrence, 26 COMPUT. LAW & SEC. REV. 298, 300 (2010).

138. *Russia "Was Behind German Parliament Hack,"* BBC (May 13, 2016), https://www.bbc.com/news/technology-36284447.

139. CASE STUD. ON THE APPLICATION OF INT'L L. IN CYBERSPACE DEP'T FOREIGN AFFS. & TRADE (AUSTL.), at 4 (February 5, 2020) https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf.; Press Release, *Statement from the Press Secretary*, WHITE HOUSE (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

Things moved faster vis-à-vis *WannaCry*, as the attack allegedly started on May 12, 2017, and attribution was officially made by the United Kingdom in October 2017.[140] At the time, though, hackers had already "cashed out on more than $143,000 worth of bitcoin."[141] In contrast, attribution of the 2020 U.S. federal government hack was made even though vulnerabilities were still being exploited,[142] and release of new security measures continued long after the authors of the Microsoft Exchange data breach had been identified.[143] It is true that Article 31 of the DARS also mentions that "the responsible state is under an obligation to make full reparation for the injury caused by the internationally wrongful act."[144] This means that victims of cyberattacks may, even if the cyberattacks have already ceased, demand reparation for the injury caused. This is difficult, though, for two main reasons. First, the cost of security breaches is not always easy to assess. Second, authors of cyberattacks have vigorously rejected the accusations made against them, even if 'attribution' had been made on the basis of sound intelligence. There is little chance that they would accept bearing any costs arising from that situation. This means that most cyberattacks will remain unpunished – and without a proper reparation. As of today, most victims of cyberattacks have been unable to react, and some of them decided to do so in a clandestine manner. Following *NotPetya*, Ukraine quickly blamed Russia, but concrete measures were not reported.[145] Even if the White House called it "a reckless and indiscriminate cyberattack" that "will be met with international consequences," no further response was reported either.[146] It was the same for the United Kingdom, as the Foreign

140. Ryan Browne, *UK government: North Korea was behind the WannaCry cyber-attack that crippled health service*, CNBC (Oct. 27, 2017), https://www.cnbc.com/2017/10/27/uk-north-korea-behind-wannacry-cyber-attack-that-crippled-nhs.html [hereinafter Browne, *North Korea*].

141. Ryan Browne, *Hackers Have Cashed Out on $143,000 of Bitcoin From the Massive WannaCry Ransomware Attack*, CNBC (Aug. 3, 2017), https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-bitcoin-from-the-massive-wannacry-ransomware-attack.html [hereinafter Browne, *Hackers*].

142. Memorandum from the U.S. Nat'l Sec. Agency on Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials (Dec. 7, 2020), https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF [hereinafter NSA Memorandum].

143. Robert Carnevale, *Microsoft Exchange Introduces New Security Measures to Prevent Another 2021*, WINDOWS CENTRAL (Sept. 28, 2021), https://www.windowscentral.com/microsoft-exchange-introduces-new-security-measures-prevent-another-2021.

144. DARS with Commentaries, *supra* note 104, at 191.

145. Chris Duckett, *Ukraine Calls Out Russian Involvement in Petya*, Z.D. NET (Jul. 3, 2017), https://www.zdnet.com/article/ukraine-calls-out-russian-involvement-in-petya/.

146. Press Release, *Statement from the Press Secretary*, WHITE HOUSE (Feb. 15, 2018), https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ [hereinafter *Feb. 2018 Statement from the Press Secretary*].

Office Minister for Cyber Security (Lord Ahmad of Wimbledon) declared that "attack showed a continued disregard for Ukrainian sovereignty" (despite Britain's initial reluctance in applying this principle), and that "costs" would be imposed.[147] *WannaCry* did not prompt concrete measures either. Again, the United Kingdom declared that there would be "costs,"[148] while the United States acknowledged that "President Trump ha[d] used just about every lever you can use, short of starving the people of North Korea to death, to change their behavior," which meant that Washington "d[id]n't have a lot of room left here to apply pressure to change their behavior."[149] However, it is an open secret that in past situations (i.e., the hack on Sony Pictures Entertainment), the United States reacted and covertly affected the functioning of the Internet in North Korea for several days.[150]

Above, I had the opportunity to underline that states were often reluctant in applying punitive measures. However, an in-depth reading of the DARS may reveal that countermeasures are actually not punitive as long as proper reparation has not been made or that the dispute has not been brought before a court. Indeed, Article 52(3) of the DARS reads as follows: "[c]ountermeasures may not be taken, and if already taken must be suspended without undue delay if: (a) the internationally wrongful act has ceased; and (b) the dispute is pending before a court or tribunal which has the authority to make decisions binding on the parties." The comments attached to the draft conclusions make clear that these conditions are cumulative, as "[p]aragraph 3 deals with the case in which the wrongful act has ceased and the dispute is submitted to a court or tribunal which has the authority to decide it with binding effect for the parties."[151] This second condition is quite restrictive, as the court or tribunal must exist, be in a position to deal with the case, and order provisional measures.[152] Then, Article 49(1) and 53 of the DARS

147. *Foreign Office Minister Condemns Russia for NotPetya attacks*, FOREIGN AND COMMONWEALTH OFFICE (UK) (Feb. 15, 2018), https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

148. *Foreign Office Minister condemns North Korean actor for WannaCry attacks*, FOREIGN AND COMMONWEALTH OFFICE (UK) (Feb. 15, 2018), https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

149. *Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea*, WHITE HOUSE (Dec. 19, 2017), https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ [hereinafter *WannaCry Press Briefing*].

150. Dan Efrony & Yuval Shany, *A Rule Book on The Shelf: Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 538, 608-09 (2018).

151. *Report of the International Law Commission to the General Assembly*, *supra* note 33, at 136.

152. *Id*.

highlight that "[a]n injured state may only take countermeasures against a state which is responsible for an internationally wrongful act in order to induce that state to comply with its obligations under Part Two," and that "[c]ountermeasures shall be terminated as soon as the responsible state has complied with its obligations under Part Two in relation to the internationally wrongful act." However, "obligations under Part Two" include, inter alia, an obligation of cessation and of reparation. It means that, provided that the internationally wrongful act was not subject to reparation or brought before a court, countermeasures may still be implemented. This is in line with the original meaning of the DARS, according to which "[a]ny other conclusion would immunize from countermeasures a state responsible for an internationally wrongful act if the act had ceased, irrespective of the seriousness of the breach or its consequences, or of the state's refusal to make reparation for it."[153] International courts and tribunals, for their part, affirmed that reprisals shall be taken against the provoking state,[154] and be proportional.[155]

Yet, where a group of states is interested in responding to a cyberattack against one member, there is another controversy, as the possibility to resort to the so-called "collective countermeasures" is disputed.[156] The DARS does not reach a definitive conclusion on this point, and the ILC decided to create a saving clause which reserves the position and leaves the resolution of the matter to the further – owing to the fact that "the current state of international law on countermeasures taken in the general or collective interest [was] uncertain" and that "there appear[ed] to be no clearly recognized entitlement of states" to take countermeasures in the collective interest.[157] Article 48 of the DARS nevertheless reserved the possibility to invoke responsibility to protect another injured state where the obligation breached is owed to "a group of states including that state, and is established for the protection of a collective interest of the group" or "to the international community as a whole." In the opinion of the ILC, examples of the former include the environment or security of a region, like a regional nuclear-free-zone

153. *Id.* at 131; *See also* TALLINN, *supra* note 132, at 116-18; DELERUE *supra* note 32, at 448.

154. Execution of German-Portuguese Arbitral Award of June 30th, 1930 (Germany, Portugal) 3 U.N.R.I.A.A. 1371 (1933).

155. Air Service Agreement of 27 March 1946 between the United States of America and France 18 U.N.R.I.A.A. 417 (1978).

156. Denis Alland, *Countermeasures of General Interest*, 13 EUR. J. UNT'L L. 1221, 1233 (2002).

157. James Crawford (Special Rapporteur), *Third Rep. on State Resp.*, at 105, U.N. Doc. A/CN.4/507 (2000); *See also* Przemysław Roguski, *Collective Countermeasures in Cyberspace – Lex Lata, Progressive Development or a Bad Idea?*, *in* 20/20 VISION: THE NEXT DECADE 5, 30 (Tatiana Jančárková et al. eds., 2020).

treaty or a regional system for the protection of human rights, and they are not limited to arrangements established only in the interest of the member states but would also extend to agreements established by a group of states in some wider common interest.[158] Special Rapporteur James Crawford added that the rules about the use of force created collective and erga omnes obligations.[159] However, most cyberthreats described above are below use of force, and – apart from NATO, which would authorize a collective reaction in the event of an external armed attack – there are few security obligations of this nature.[160] It thus seems that most cyberthreats do not currently appear as a breach of a collective interest, which would justify collective countermeasures,[161] and do not breach erga omnes obligations either.[162]

## IV. RESOLVING THE CHALLENGES IN BUILDING DETERRENCE-BY- PUNISHMENT ON THE DOCTRINE OF COUNTERMEASURES

The ingredients of a proper deterrence policy typically involve the capacity to inflict consequences where rules are infringed by a foreign actor,[163] as well as credibility: the latter must indeed believe that the threat of retaliation is real.[164] If such policy was to be defined at the EU scale, various steps are required. First, European states must adopt a common approach to the application of existing rules (4A). Second, common attribution is required (4B). Both conditions are indeed required to determine the existence of an internationally wrongful act and, eventually, resort to countermeasures. This would pave the way for a common deterrence policy (4C).

### *A. Common Primary Rules*

Even if a specific tool for the regulation of cyberspace might be a better solution than the application of existing rules – owing to the fact that new technologies might not be analogous to prior cases[165] – the creation of a new binding treaty about cyberoperations is an unlikely

158. INT'L L. Comm'n, Rep. on the Work of Its Sixty-Third Session, *supra* note 37 at 126.
159. Crawford, *supra* note 157, at 105.
160. *Id*.
161. Roguski, *supra* note 157, at 36-7.
162. *Id*. at 32.
163. THOMAS SCHELLING, ARMS AND INFLUENCE 42 (rev. Ed. 2008).
164. Geers, *supra* note 137, at 300.
165. Duncan Hollis, *The Fog of Technology and International Law*, SIDIBLOG (May 14th, 2015), https://www.sidiblog.org/2015/05/14/the-fog-of-technology-and-international-law.

scenario, and has received little support.[166] As far as other instruments are concerned, most Asian states did not endorse proposals like the *Paris Call for Trust and Security in Cyberspace*.[167] Conversely, the *International Code of Conduct for Information Security* designed by China Russia and several Central Asian Republics did not generate much enthusiasm.[168] Experts have demonstrated that states engage in the process of international decision making out of self-interest, and that treaties may be described as the product of mutual benefits and customary law as well as coincidence of interest.[169] Today, there is no coincidence of interest, and one can doubt that it will occur soon. Thus, at present, the interpretation of existing rules might be the best option if one wants to achieve some regulations of cyberthreats. However, as explained above, the European Union made a regrettable choice in this context: the Cyber Diplomacy Toolbox did not clearly define what was unlawful and what was unfriendly. It is interesting to note that, following discussions with members of the Organization of American States (OAS), Duncan Hollis identified several reasons why states may remain silent in that respect[170] First, he explained that – due to the relative novelty of cybersecurity and the lack of governmental expertise and resources – states sometimes may not be able to formulate an opinion on the application of international law.[171] In some cases, he noted that expertise indeed existed, but was "distributed in ways that make it difficult to coalesce into a formal state view that can be expressed publicly."[172] Second, he underlined that some states wanted to "retain freedom to engage in cyberoperations."[173] Hence, there could be "a reluctance to take positions on what operations

166. *Comments from Italy on the Initial 'Pre-Draft' Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunication in the Context of International Security*, at 3 U.N. OFF. FOR DISARMAMENT AFFS. (Apr. 16, 2020), https://front.un-arm.org/wp-content/uploads/2020/04/2020-04-16-italy-comments-on-the-oewg-pre-draft.pdf [hereinafter Italy Comments on OEWG].

167. The supporters, (Nov. 12, 2018), https://www.pariscall.international/en/supporters; Sarah McKune, An Analysis of the International Code of Conduct for Information Security, (Sept. 28, 2015), https://www.citizenlab.ca/2015/09/international-code-of-conduct/.

168. *Id*.

169. JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW 225 (2005).

170. Duncan Hollis, *Improving Transparency: International Law and State Cyber Operations – Fifth Report*, *in* INTER-AMERICAN JUDICIAL COMMITTEE INTERNATIONAL LAW AND STATE CYBER OPERATIONS, at 15, OEA/Ser.Q CJI/doc.603/20 Rev.1Corr.1, (Nov. 1, 2020), https://www.oas.org/en/sla/iajc/docs/International_Law_and_State_Cyber_Operations_publication.pdf [hereinafter *International Law and State Cyber Operations – Fifth Report*].

171. *Id.* at 15-16.

172. *Id.*

173. *Id.*

international law might prohibit or restrict lest that limit their future freedom to maneuver or react."[174] Third, he reported that powerful actors like China, Russia, and the United States had taken "discrete" and "often conflicting" views on the regulatory role of international law.[175] For this reason, "[s]ome member states indicated a reluctance to make similar signals lest they embroil that state in the competition and conflict among these actors; issues states can avoid by staying silent."[176] These findings may well be valid in Europe, where offensive and defensive cybercapacities vary from one state to another, as well as resources and bilateral relations with some of the actors mentioned above. However, a common understanding would have permitted the Union to denounce a breach of international law whenever it occurred, put the blame on a foreign nation – and eventually, allow member states to retaliate. What's more, it is arguable that "stop[ping] short or leav[ing] their views ambiguous' would 'only encourage further malicious activities by aggressive states."[177] It means that – in the event of a cyberattack – governments should clearly articulate what international law rules are considered breached. In fact, some politicians – like the late U.S. Senator John McCain – previously acknowledged that a first step in the development of a deterrence policy consisted of figuring out what cyberthreats should be viewed as being contrary to international law.[178]

As the effects of those cyberoperations are usually below the threshold of the use of force and are not coercive, states may perhaps seek refuge in sovereignty.[179] In fact – and in spite of the apparent divergences on that issue – a consensus may not be unachievable at the European scale. First, it seems that member states usually view sovereignty as an international rule *per se*, which applies in cyberspace.[180] Second, they

174. *Id.*

175. *Id.*

176. *Id.*

177. Przemysław Roguski, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, JUST SECURITY (Mar. 6, 2020), https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/ [hereinafter *Russian Cyber Attacks*].

178. *Intel Chiefs Testify on Russian Hack*, *supra* note 63, at 8.

179. See Roguski, *supra* note 157, at 30. *See also* Michael Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum*, 8 HARV. NAT'S SEC. J. 239, 257 (2017).

180. This was the view adopted by Estonia, Germany, Norway and Romania. *See* Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established

already agreed that cyberattacks, which result in material harm or physical effects, may breach sovereignty. At present, they may go one step further, and acknowledge that cyberattacks which result in the loss of data or functionality and are sufficiently serious, would indeed be contrary to this rule.[181] In addition, the very states that are suspected of carrying out cyberattacks – and refused to endorse previous attempts at defining specific norms like the Paris Call – often agree that sovereignty is relevant in cyberspace. This is the case for China, who considered that – by virtue of sovereignty – no country should "engage in, condone or support cyberactivities that undermine other countries' national security."[182] It is the same for Iran, who mentioned that "[a]ny utilization of cyberspace, if and when involves unlawful intrusion to the (public or private) cyberstructures which is under the control of another state, may constitute as a violation of the sovereignty of the targeted state."[183] If states still disagree about the meaning of sovereignty, reshaping their approach to due diligence might be a valuable alternative. As underlined above, this principle may be subject to different interpretations: it may mean that states shall not tolerate – and from their own territories – the perpetration of wrongful acts and/or transboundary harm.[184] Member states may agree that due diligence is breached whenever another state tolerates that an actor, who is active on one's own territory, perpetrates a wrongful act or causes more than de minimis harm abroad (whether physical, virtual, functional or financial).[185] For instance, when China was suspected of having exploited the vulnerabilities of Microsoft Exchange

Pursuant to General Assembly Resolution73/266, UN Doc. A/76/136, at 24-5, 33, 67, 76 (2021) [hereinafter Official Compendium of Voluntary National Contributions].

181. This would exclude de minimis effects, such as the disabling of a firewall or the installation of a backdoor. For example, *see* German Federal Government, *supra* note 81, at 7.

182. *International Strategy of Cooperation on Cyberspace*, CHINESE MINISTRY OF FOREIGN AFFAIRS (2017), https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html [hereinafter China's International Strategy of Cooperation on Cyberspace].

183. *Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace*, ALDIPLOMASY (2020), https://www.aldiplomasy.com/en/?p=20901.

184. A more stringent position adopted by Rule 6 of the Tallinn Manual 2.0 refers to 'cyber operations that affect the rights of, and produce serious adverse consequences for, other states'. *See* TALLINN, *supra* note 132, at 30.

185. Some experts elaborated on liability in the event of cyberattacks. *See* Beatrice Walton, *Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Tort in International Law*, 126 YALE L.J. 1460, 1505-06 (2017); Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 606 (2018); Akiko Takano, *Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications*, 36 LAWS 7 (2018).

email servers, Rachel Noble – the Director-General of the Australian Signals Directorate (ASD) – declared:

> [t]o explain it in plain language, it would be like houses or buildings having faulty locks on the doors . . . when the Chinese government became aware of the faulty locks on the doors, they went in and they propped all those doors open . . . [t]here was opportunity for all sorts of criminals, other state actors . . . to pour in behind those propped-open doors and get into your house or your building.[186]

She added, "[this action] crossed a line in the judgment of policy agencies and governments around the world," was "reckless," and "should not be tolerated as a matter of international and global norms."[187] Yet, due diligence may be well-suited to tackle this type of situation. In contrast, following the hack on the Colonial Pipeline, U.S. President Biden emphasized that, ". . . we do not believe the Russian Government was involved in this attack. *But* we do have strong reason to believe that the criminals who did the attack are living in Russia. . . ." [188] For this reason, he also declared:

> [w]e have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks . . . [w]e are working to try to get to the place where we have sort of an international standard that governments knowing that criminal activities are happening from their territory, that we all – we all move on those – those criminal enterprises.[189]

Again, this may be aligned with what is expected under due diligence. It is arguable, then, that if Moscow was not directly responsible for the attack, it must at least take action against the hackers who are based in the territory of the Russian Federation. If the Kremlin fails to do

186. Andrew Tillett, *China 'Crossed Line' with Email Cyberattack, Cybersecurity Tsar Says*, FIN. REV. at 2 (July 29, 2021), https://www.afr.com/politics/federal/china-crossed-line-with-email-cyberattack-cyber-security-czar-says-20210729-p58e0x.

187. *Id*.

188. Remarks on the Colonial Pipeline Ransomware Attack and an Exchange With Reporters, 2021 DAILY COMP. OR PRES. DOC. 202100402 at 2 (May 13, 2021).

189. *Id.* at 2-3. President Biden also declared that the United States was "going to pursue a measure to disrupt their ability to operate" and did not exclude "retaliatory cyberattacks to shut down these criminals." If the Russian government had no ties with the hackers, it would probably not be acceptable.

that, this will amount to a breach of due diligence. Unfortunately, most states are divided over the interpretation of due diligence,[190] but the adoption of the third approach underlined above would be well-suited to address these foreign cyberthreats.

### *B. Common Attribution*

Attribution is a multidimensional process, with legal, forensic, technical and political aspects,[191] which has sometimes been described as a "messy and decentralized" regime.[192] To establish a link between a cyberattack and a state, both the computers and networks used, and the human operator who carried it out (technical and forensic dimensions) must be identified.[193] If a given cyberattack is wrongful and a state was behind the operation, then attribution is possible from a legal point of view (legal dimension). However, attribution is also a sovereign political decision which is adopted with due consideration for the broader context (political dimension).[194] It must be noted that these questions are of great sensitivity for national sovereignty, and that a "lack of mutual trust pushes EU member states to tackle cyber issues on their own rather than conceive it as an EU competence."[195] In addition, states are usually reluctant in sharing intelligence materials, as "sensitive information about sources or tools used to gather that evidence" could be compromised.[196] For instance, Finland made clear that:

190. The first approach (wrongful act) was supported by Australia, France, Germany and Israel: AUSTLS. INT'L CYBER AND CRITICAL TECH. ENGAGEMENT STRATEGY, DEP'T FOREIGN AFFS. & TRADE (AUSTL.) at 96-100 (2021), https://www.dfat.gov.au/publications/international-relations/international-cyberengagement-strategy/aices/chapters/annexes.html#Annex-A; French Ministère des Armées, *supra* note 75, at 8; German Federal Government, *supra* note 81, at 11; Schöndorf, *supra* note 83, at 403-04. The second approach (transboundary harm) was supported by Finland. Fin Gov't, *supra* note 75, at 4; It seems that the Netherlands, Italy and Romania think that they are cumulative: Neth. Gov't, *supra* note 75, at 4-5; IT. MINISTRY OF FOREIGN AFFS., ITALIAN POSITION PAPER ON INTERNATIONAL LAW & CYBERSPACE, at 7 (2021), https://www.esteri.it/MAE/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf [hereinafter ITALIAN POSITION PAPER]; Official Compendium of Voluntary National Contributions, *supra* note 180, at 76.

191. Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 527-29 (2020); GUARDIAN OF THE GALAXY, *supra* note 95, at 52.

192. Eichensehr, *supra* note 191, at 526.

193. GUARDIAN OF THE GALAXY, *supra* note 95, at 53.

194. *Id.* at 67.

195. Constant Pâris, *Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace* (Coll. Of Eur. Dep't. of EU Int'l. Rels. & Dipl. Stud., Working Paper, 2021).

196. Erica Moret & Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: Towards A Cyber Sanctions Regime?*, EUR. UNION INST. FOR SEC. STUD. (July 12, 2017), https://www.iss.europa.eu/content/eu-cyber-diplomacy-toolbox-towards-cyber-sanctions-regime; Moreover,

> [t]here is no general obligation for a state taking countermeasures to disclose the information on the basis of which the action is taken. At the same time, it is in each state's best interests to ensure that a decision to take countermeasures is based on solid evidence, given that recourse to countermeasures would otherwise constitute an internationally wrongful act. A state that responds to a hostile cyberoperation must therefore have adequate proof of the source of the operation and convincing evidence of the responsibility of a particular state.[197]

In fact, it is arguable that full transparency vis-à-vis third states and European partners is neither realistic nor necessary.[198] On the one hand, countries like China and Russia "have a strong interest in forcing accusing countries to disclose as much information as possible since doing so often reveals sources and methods used by law enforcement and the intelligence community."[199] On the other hand, European states may well have common interests in terms of international security, but have divergent ones and remain competitors on the economic sphere. It is not a secret that European states sometimes spy on each other to acquire trade secrets,[200] and that Denmark was recently described as "the NSA's listening post in Europe."[201] In addition, the bilateral relations of Europeans with "hacker states" are not the same. A recent press report underlined, for instance, that "Hungary under Viktor Orban has become one of the most China-friendly EU countries, repeatedly preventing the European Union from adopting critical remarks on China (which require consensus among the bloc's members)."[202] Indeed, this type of decision is adopted in the framework of the CFSP which has a special position in the

'[d]ocumenting the accusation thus risks giving the accused or third parties information that can be used to degrade future investigative efforts. They may even create new opportunities for offensive cyberoperations'. *See* Finnermore & Hollis, *supra* note 25, at 988.

197. Fin. Gov't, *supra* note 75, at 6.

198. Eichensehr, *supra* note 191 at 569.

199. *Id.* at 545.

200. Giliam de Valk, *Mind the Gap: Economic Espionage within the EU*, INST. OF SEC. AND GLOB. AFFS. (Nov. 20, 2017), https://www.leidensecurityandglobalaffairs.nl/articles/mind-the-gap-economic-espionage-within-the-eu.

201. Sébastien Seibt, *How Denmark Became the NSA's Listening Post in Europe*, FRANCE 24 (June 1, 2021), https://www.france24.com/en/technology/20210601-how-denmark-became-the-nsa-s-listening-post-in-europe.

202. Richard Q. Turcsanyi & Matej Šimalčík, *Hungarian Policy Toward China Might Be Facing a Seismic Shift*, THE DIPLOMAT (June 9, 2021), https://www.thediplomat.com/2021/06/hungarian-policy-toward-china-might-be-facing-a-seismic-shift/.

EU's legal order as it is "[d]efined in clearly inter-governmental terms" (i.e., the dominant role of unanimous voting and the near exclusion from the jurisdiction of the ECJ).[203] The Common Security and Defense Policy (CSDP) – which is an integral part of the CFSP – may also be used "on missions outside the Union for peace-keeping, conflict prevention and international security strengthening."[204] In this context, the civilian and military capabilities of member states are made available to the Union.[205] In addition, there are sizable differences between member states when it comes to national capacities in the field of cyberdefense.[206] In fact, the European Commission acknowledged that "[m]ember states have the primary responsibility for the response in case of large scale cybersecurity incidents or crises affecting them" – even if the European Union had "an important role, stemming from Union law or from the fact that cybersecurity incidents and crises may impact all sections of economic activity within the Single Market, the security and international relations of the Union, as well as the institutions themselves."[207] There may be some ways, however, to reconcile this concern and a collective approach in the framework of the CFSP. In situations where the European Union is subject to an external cyberattack – and once the human perpetrator has been identified – member states may decide that there is sufficient proof to establish that a third state was behind the operation (or tolerated it) and delegate the power to respond on behalf of all member states to the most capable European states.[208] There is only a short step between placing the blame on a foreign intelligence service and on the state itself. Indeed, Article 7 of the DARS clearly mentions that:

> [t]he conduct of an organ of a state or of a person or entity empowered to exercise elements of the governmental authority shall be considered an act of the state under international law if

203. Panos Koutrakos, *External Action: Common Commercial Policy, Common Foreign and Security Policy, Common Security and Defense Policy in* THE OXFORD HANDBOOK OF EUROPEAN UNION LAW 271 (Anthony Arnull & Damian Chalmers eds., 2015).

204. Consolidated Version of the Treaty on European Union art. 42(1), Feb. 7. 1992, 2012 O.J. (C 326) 38 [hereinafter TEU 42(1)].

205. Consolidated Version of the Treaty on European Union art. 42(3), Feb. 7. 1992, 2012 O.J. (C 326) 38.

206. Helena Carrapico & André Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, 55 J. COMMON MKT. STUD. 1254, 1254-65 (2017).

207. *Commission Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises*, at 4, COM (2017) 6100 final (Sept. 13, 2017) [hereinafter *Cybersecurity Incidents and Crises*].

208. An interesting proposal was made by Zach West, who suggested that a 'deputy relationship' between the government and private companies may be defined. West, *supra* note 49, at 140.

> the organ, person or entity acts in that capacity, even if it exceeds its authority or contravenes instructions.

The Joint Cyber Unit –[209] which is not entitled to take unilateral actions – might help coordinate their actions.[210]

### *C. Common Deterrence Policy*

Where deterrence by punishment is contemplated, credibility is essential, and it "depends both on the ability and the will of the defender to retaliate."[211] Above, I had the opportunity to demonstrate that countermeasures may indeed not be punitive, but also that countermeasures did not qualify as punitive as long as proper reparation had not been made, or that the dispute had not been brought to a jurisdiction. If this is not the case, countermeasures are available. For instance, this is what emerges from Estonia's position: "[i]n order to enforce state responsibility, states maintain all rights to respond to malicious cyberoperations in accordance with international law . . . The main aim of reactive measures in response to a malicious cyberoperation is to ensure responsible state behavior in cyberspace and the peaceful use of ICTs."[212] It is particularly interesting to note that under this perspective, prevention and reaction are intertwined. It is equally interesting to note that a couple of states departed from some of the ILC's draft conclusions as far as cyberspace is concerned, thus relaxing certain limitations on countermeasures.[213] For instance, Israel, the United Kingdom and the United States did not agree that it is compulsory to give prior notification before taking countermeasures against hostile states.[214] Even though notification is not required in situations where "urgent countermeasures" are "necessary to preserve [the injured state's] rights," the explanation given by the United Kingdom was a different one:

---

209. European Commission Press Release IP/21/3088, EU Cybersecurity: Commission proposes a Joint Cyber Unit to Step Up Response to Large-Scale Security Incidents (June 23, 2021).

210. *Why the Time is Ripe for an EU Joint Cyber Unit: Interview with Patrick Calvar*, IINSTITUT MONTAIGNE, (July 21, 2021), https://www.institutmontaigne.org/en/analysis/why-time-ripe-eu-joint-cyber-unit [hereinafter *Interview with Patrick Calvar*].

211. Aaron Brantly, *Entanglement in Cyberspace: Minding the Deterrence Gap*, 16 Democracy & Sec. 210, 211 (2020).

212. Official Compendium of Voluntary National Contributions, *supra* note 180, at 28.

213. Gary Corn & Eric Jensen, *The Use of Force and Cyber Countermeasures*, 32 TEMP. INT'L. L.J. 127, 127-133 (2018).

214. Jeremy Wright, *supra* note 75; Schöndorf, *supra* note 83, at 405.

> [t]he covertness and secrecy of the countermeasures must of course be considered necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.[215]

In addition, it appears that prior notification would enable the responsible state to prevent or mitigate a cyber countermeasure, and would make it "far less effective in encouraging compliance and protecting the victim state."[216]

Against this background, the next question is about the modalities of a response. The challenge is that it must be sufficiently deterrent, but without resulting in escalation. For this reason, proportionality requires that "[c]ountermeasures must be commensurate with the injury suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[217] However – and save some exceptions – victims are free to determine how they will respond, and what obligations normally owed to the author may be deviated from. As countermeasures shall not involve the use or the threat to use force, deterrence by punishment may never be built on the perspective that cyberattacks which are below the use of force will be answered with measures which are above this threshold. Even if the use of kinetic weapons to answer cyberattacks was not ruled out by some states, this could only be contemplated where the latter amounted to the use of force.[218] One may fear that a physical response to counter cyberattacks which are below the use of force could be at odds with the UN Charter, and would result in escalation.[219] For this reason, the intermediary position would probably consist in responding

---

215. *Id*.

216. They further underline that "[u]nlike conventional weapons that are often destroyed when used, cyber tools can be captured and reused or retooled, even after they are employed. States have a significant aversion to compromising unique cyber capability under any circumstances and, because doing so would diminish the effectiveness of the cyber tool, such potentially compromising notification is even less likely to happen willingly." *See* Corn & Jensen, *supra* note 213 at 131. An alternative suggested by other experts consists in considering that notice has already been given for states who systematically violate their obligations: Messerschmidt, *supra* note 114, at 320.

217. DARS with Commentaries, *supra* note 105, at 134.

218. Egan, *supra* note 131, at 178; *National Cyber Strategy of the United States of America*, NAT'L SEC. COUNCIL, 21 (Sep. 20, 2018), https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf ; AUSTLS. INT'L CYBER AND CRITICAL TECH. ENGAGEMENT STRATEGY, *supra* note 190, at 98; German Federal Government, *supra* note 81, at 13; French Ministère des Armées, *supra* note 75, at 8; Jeremy Wright, *supra* note 75.

219. AUSTLS. INT'L CYBER AND CRITICAL TECH. ENGAGEMENT STRATEGY, *supra* note 190, at 98; Fin. Gov't, *supra* note 75, at 6; Halberstam, *supra* note 62, at 210-213.

to digital attacks with digital attacks. However, it shall not be required to answer to a cyberattack with the very same type of cyberattacks. In fact, "different actors require different types of deterrence."[220] Hacking pipelines, power plants or companies would not necessarily be relevant in that context. This means that adequate responses would aim at what one values the most – i.e., one's own Achilles' Heel. In the case of China, the capacity to gather information and to curb internal opposition is valued.[221] This means, then, that:

> the loss of the ability to monitor China's population, damage to the various information networks that support censorship of traditional media, monitor social media, and limit access to the outside world, would be as devastating as the American inability to detect missile launches or guide JDAMs [Joint Direct Attack Munitions].[222]

The Russian government is also afraid of regime change.[223] In a nutshell, opening up breaches in the censorship and monitoring systems of these countries, like the Great Firewall, would pressure countries in their "Achilles' Heel." In addition, the main objectives of hackers are often no secret. North Korea is in desperate need for cash,[224] China is interested in gathering intellectual property[225] and information about ethnic minorities and political dissidents,[226] while Russia tries to influence the politics in other states.[227] Thus, a proper deterrence policy could seemingly be combined to better cyberdefense. However, merely

220. BUCHANAN, supra note 61, at 149. *See also* Richard L. Kugler, *Deterrence of Cyber Attacks*, *in* CYBERPOWER AND NATIONAL SECURITY 309, 327 (Franklin D. Kramer, et. al. eds., 2009); Talbot Jensen, *supra* note 48, at 782.

221. DEAN CHENG, CYBER DRAGON: INSIDE CHINA'S INFORMATION WARFARE AND CYBER OPERATIONS 219 (2017).

222. *Id*. at 219.

223. Leonid Bershidsky, Opinion, *Russian Generals' Biggest Fear? Ordinary Russians*, MOSCOW TIMES (Mar. 4, 2019), https://www.themoscowtimes.com/2019/03/04/what-scares-russias-generals-the-most-russians-a64703.

224. Ed Caesar, *The Incredible Rise of North Korea's Hacking Army*, NEW YORKER (May 3, 2021), https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.

225. Nicole Perlroth, *How China Transformed Into a Prime Cyber Threat to the U.S.*, N.Y. TIMES, https://www.nytimes.com/2021/07/19/technology/china-hacking-us.html?smid=url-share (last updated July 20, 2021).

226. Nicole Perlroth et al., *China Sharpens Hacking to Hound Its Minorities, Far and Wide*, N.Y. TIMES, https://www.nytimes.com/2019/10/22/technology/china-hackers-ethnic-minorities.html?smid=url-share (last updated Dec. 9, 2020).

227. Brewster, *supra* note 11, at 1.

undermining the anonymity of hackers appears insufficient in discouraging foreign hackers.[228] As former U.S. President Barack Obama declared about Russia, "[i]t is not like . . . Putin's going around the world publicly saying look what we did, it wasn't that clever. He denies it. So, the idea that somehow public shaming is going to be effective, I think doesn't read the thought process in Russia very well."[229]

In the opinion of some experts, deterrence in cyberspace could not be achieved, due to the likeliness of collateral damage, difficulties in attribution, asymmetry, and the lack of credibility.[230] However, some of these fears may be excessive. First, the recent history of cyberattacks reveal that targeted actions in cyberspace may be taken and do not always result in significant collateral damage.[231] Second, as highlighted with the examples of successful attribution above, this process is now easier than it used to be. Third, it is true that "some countries are more dependent upon the Internet than others" and that "[s]ome governments possess sophisticated computer network attack programs while others have none at all."[232] However, as suggested above, there are different costs that the victims of cyberattacks may inflict to hostile actors, including the disruption of their domestic surveillance and censorship capabilities. It means that, even though these states are less dependent upon the Internet than others, significant costs may still be inflicted on the assets they value. In fact, it appears that the fourth criticism – i.e., the lack of credibility – may be the main problem. The difficulty is not so much about transparency, that is, showing other states one's own capacities, the vulnerabilities that one is able to exploit and the techniques that one is able to use. It is arguable, anyway, that their specific nature would often evolve and that technologically advanced states will have the means to discover new vulnerabilities and to inflict costs.[233] The main problem, so

228. Contra Cornish, *supra* note 29, at 14; Adam Rodrigues, *If the Law Can Allow Takebacks, Shouldn't It Also Allow Hackbacks?*, 24 MARQ. INTELL. PROP. L. REV. 1, 12 (2020).

229. *Full Transcript: President Obama's Final End-of-Year Press Conference*, POLITICO (Dec. 16, 2016, 6:00 PM), https://www.politico.com/story/2016/12/obama-press-conference-transcript-232763 [hereinafter *Obama Press Conference*].

230. BRANDON VALERIANO & RYAN MANESS, CYBER WAR VERSUS CYBER REALTIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM 47 (Oxford Univ. Press, 2015); Geers, *supra* note 137, at 301.

231. *Significant Cyberincidents*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited Oct. 18, 2022).

232. Geers, *supra* note 137, at 302.

233. *Id.* at 300; *see* Talbot Jensen, *supra* note 48, at 788 (As Eric Talbot Jensen put it, "unlike many kinetic weapons, most cyber weapons are "single use" weapons. In other words, using a cyber tool, or even displaying it, may make it ineffective . . . Once the defects were used, they became known, and "patches" were issued which prevented those same exploits from being issued again.

it seems, resides in the will to inflict such costs. For instance, the United States likely has capacity to retaliate in cyberspace, and it already responded to cyberattacks carried out by North Korea. However, it only threatened Russia (more rarely China) in some cases, without taking concrete action, even when the U.S. government was urged to do so. It may well be that Moscow and Beijing doubt that victims will dare to strike one day, which is problematic in a deterrence context. In addition, and even though several states have counterattack capacities, few of them have openly argued in favor of deterrence.[234] The United Kingdom and the United States are among the few exceptions. After the *WannaCry* attacks, the British Secretary of State for Defense declared that the "doctrine of deterrent," which would be similar to nuclear dissuasion, was required.[235] He added that the United Kingdom had "a counterattack capability" but that attention needed to be given to the "tit-for-tat" scenario and to the risk Britons would be exposed to.[236] Observers noted that he "stopped short of suggesting the United Kingdom could carry out retaliatory attacks."[237] In 2016, James Clapper, the former Director of National Intelligence, argued that the United States "cannot put a lot of stock . . . in cyberdeterrence. Unlike nuclear weapons, cybercapabilities are difficult to see and evaluate and are ephemeral. It is accordingly very hard to create the substance and psychology of deterrence . . . ."[238] However, the tone changed in 2018. Washington made clear:

> [a]s the United States continues to promote consensus on what constitutes responsible state behavior in cyberspace, we must also work to ensure that there are consequences for irresponsible behavior that harms the United States and our partners. All instruments of national power are available to prevent, respond to, and deter malicious cyberactivity against the United States.[239]

---

In this way, signaling a cyber weapon often makes it ineffective, which is seldom the case with standard kinetic weapons.")

234. TALLINN, *supra* note 132, at 30.

235. Adam Withnall, *British Security Minister Says North Korea Was Behind WannaCry Hack on NHS*, INDEPENDENT (Oct. 27, 2017, 9:30 AM), at https://www.independent.co.uk/news/uk/home-news/wannacry-malware-hack-nhs-report-cybercrime-north-korea-uk-ben-wallace-a8022491.html.

236. *Id.*

237. *Id.*

238. *Intel Chiefs Testify on Russian Hack*, *supra* note 63, at 8. *See also* Eric Myjer, *Some Thoughts on Cyber Deterrence and Public International Law*, in RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 284, 303-304 (Nicholas Tsagourias & Russell Buchan eds., 2015).

239. *National Cyber Strategy of the United States of America*, *supra* note 219, at 21.

In November 2021, the United Kingdom and the United States agreed to address foreign cyberthreats by "planning enduring combined cyberspace operations that enable a collective defense and deterrence and impose consequences on our common adversaries who conduct malicious cyberactivity."[240] If the fear of escalation is clear in several state publications,[241] the whole point of unity resides in discouraging adversaries from shooting first – or from shooting again. This need had apparently not escaped the attention of Washington, who underlined that, "[t]he United States will formalize and make routine how we work with like-minded partners to attribute and deter malicious cyberactivities with integrated strategies that impose swift, costly, and transparent consequences when malicious actors harm the United States or our partners."[242] European states may therefore elaborate a common deterrence strategy, and convey the message that serious cyberattacks will be subject to retaliation. In this process, the doctrine of countermeasures may be of help. However, states shall insist on its dissuasive role, as they did in the framework of the *travaux préparatoires* of the DARS.

As highlighted above, another difficulty in the achievement of a common system of deterrence by punishment resides in the lawfulness of collective countermeasures. Even if it is clear that a collective answer would usually be more dissuasive than an individual one, the lawfulness of such action is still disputed. Some states, like France, argue that "[c]ollective countermeasures are not authorized, which rules out the possibility of France taking such measures in response to an infringement of another State's rights."[243] In contrast, Estonia advocated for collective countermeasures against unlawful cyberoperations "where diplomatic action is insufficient, but no lawful recourse to use of force exists," and

240. *UK and U.S. Intelligence Chiefs Commit to Enduring Combined Cyber Operations*, GOV'T. COMMC'NS. HEADQUARTERS (UK) (Nov. 18, 2021), https://www.gchq.gov.uk/news/cyber-management-review-2021 [hereinafter *UK and US Combined Cyber Operations*]

241. Neth. Gov't, *supra* note 76, at 9; AUSTRALIA'S CYBER SECURITY STRATEGY 2020, GOV'T. DEP'T HOME AFFS. (AUSTL.) 26 (Aug. 6, 2020), https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-cyber-security-strategy-2020. ; *Cyber Strategy for Germany 2016*, ENISA, at 31 (2016), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en.

242. *National Cyber Strategy of the United States of America*, *supra* note 218, at 21.

243. French Ministère des Armées, *supra* note 75, at 7. François Delerue nevertheless describes 'the creation of a right of collective countermeasures' as 'one of the likeliest evolutions of the international law applicable to cyber operations;' DELERUE, *supra* note 32, at 456.

underlined that, "[a]llies matter also in cyberspace."[244] This position was reaffirmed in the 2021 Official Compendium, which stated that:

> [i]n order to enforce state responsibility, states maintain all rights to respond to malicious cyberoperations in accordance with international law. If a cyberoperation is unfriendly or violates international law obligations, injured states have the right to take measures such as retorsions, countermeasures or, in case of an armed attack, the right to self-defense. These measures can be either individual or collective.[245]

Owing to the lack of clarity in the field and the need for interpretation, European states may still agree with Estonia on this question. As underlined above, the DARIO does not provide guidelines about the measures that international organizations are entitled to adopt when a non-member state commits an internationally wrongful act. For this reason, even if decisions to retaliate were decided at the EU level, the status of the Union as an independent legal person would not afford, at first sight, a work-around on the question of collective countermeasure.

## V. CONCLUDING THOUGHTS

In the *Art of War*, the ancient Chinese strategist Sun Tzu contended that "supreme excellence consists in breaking the enemy's resistance without fighting."[246] So far, however, neither fear of escalation nor self-restraint have discouraged foreign nations, including China, Russia and North Korea, from launching cyberattacks. In fact, authors like Robert Epstein had the opportunity to underline that, once a gap in law and order is detected, some individuals are eager to take advantage and will embolden others to do the same, which eventually results in disorder.[247] In a similar fashion, Jack Goldsmith argued twelve years ago that "[e]vents of the last decade have shown that, in the absence of concrete retaliation, complaints and vague threats will only embolden our adversaries."[248] Indeed, "[w]hen we overtly signal . . . that we have no

244. Kersti Kaljulaid, *supra* note 75, at 4.

245. Official Compendium of Voluntary National Contributions, *supra* note 180, at 28.

246. SUN TZU ON THE ART OF WAR: THE OLDEST MILITARY TREATISE IN THE WORLD 8 (Lionel Giles trans., Allandale Online Publ'g ed. 2000).

247. Richard A. Epstein, *The Theory and Practice of Self-Help*, 1 J. L. ECONS. & POL'Y 1, 1-2 (2005).

248. Jack Goldsmith, *The Insidious Cyberthreat that Goes Unreported*, WASH. POST (Nov. 25, 2011), https://www.washingtonpost.com/opinions/the-insidious-cyberthreat-that-goes-unreported/2011/11/25/gIQAKXdIxN_story.html.

tools to counteract their cyberattacks, we invite more attacks . . . ."[249] The doctrine of countermeasures may actually help in building deterrence by punishment. The *travaux préparatoires* reveals that countermeasures were also contemplated as a dissuasive tool. In addition, the non-punitive nature of countermeasures only means that there are two situations where they shall not be taken — or must cease. The first situation is where the internationally wrongful act has ceased and "the dispute is pending before a court or tribunal which has the authority to make decisions binding on the parties." The second situation is where the internationally wrongful act has ceased, and that proper reparation has been made.[250] There are two main difficulties in this context. The first is legal in nature: what counts as an internationally wrongful act in cyberspace is not very clear, and it is the same for the possibility to resort to collective countermeasures. However, these obstacles are not insurmountable and may find a common answer at the EU level. The second is political in nature: deterrence must be credible, and the equilibrium of forces is not in favor of European states as long as they are taken separately. However, the costs would be higher for foreign nations if a cyberattack triggered a collective response. In this case, deterrence by punishment would work better.

One should not be naïve though, and this solution will not always be a silver bullet. First, there may be a gap in the relations between allies themselves, who may not be discouraged from conducting questionable activities against each other. A famous quote from Pierre Marion, the former director of the French General Directorate for External Security, mentioned that "[w]e are military allies, but economic competitors. Therefore, industrial espionage, even among friends, is a normal action of an intelligence agency."[251] Nevertheless, allies still have an interest in protecting common values from foreign attackers such as democracy, human rights (including the freedom of expression), and innovation.[252] In this process, playing tough may be helpful. Second, as underlined by Jack Goldsmith and Eric Posner, self-interest and the distribution of power may explain why states engage in the creation of international law, and

249. Jack Goldsmith, *The Strange WannaCry Attribution*, LAWFARE (Dec. 21, 2017), https://www.lawfareblog.com/strange-wannacry-attribution.

250. Comments & Observations A/CN.4/515, *supra* note 69, at 136.

251. CHARLES LATHROP, THE LITERARY SPY: THE ULTIMATE SOURCE FOR QUOTATIONS ON ESPIONAGE & INTELLIGENCE 208 (2004).

252. *L'affaire Pegasus Montre Parfaitement les Faiblesses de l'Europe en Matière de Cyberagressions*, LE MONDE (July 26, 2021), https://www.lemonde.fr/idees/article/2021/07/26/l-affaire-pegasus-montre-parfaitement-les-faiblesses-de-l-europe-en-matiere-de-cyberagressions_6089519_3232.html.

why, in some situations, they decide to act contrary to it.[253] It would likely still be true in a cyberspace context, and hostile actors may well decide to breach the rules in some cases, even if there is a risk that they suffer retaliation. However, fear of retaliation usually favors compliance,[254] and states would still be better off with deterrence than without it. After all, as Duncan Hollis observed, "law does not have to regulate every case or generate 100% compliance to be effective. But law should identify and regulate undesirable behavior with sufficient compliance to shape or deter future behavior."[255]

253. JACK L. GOLDSMITH & ERIC A. POSNER, THE LIMITS OF INTERNATIONAL LAW 225 (2005).

254. *Id*. at 100.

255. Duncan Hollis, *Re-Thinking the Boundaries of Law in Cyberspace*, *in* CYBER WAR: LAW & ETHICS FOR VIRTUAL CONFLICTS 129, 150 (Jens David Ohlin et al. eds., 2015).