Bergen Journal of Criminal Law and Criminal Justice • Volume 12, Issue 2, 2024, pp. 1-30.

The Role of Criminal Law Approaches Against Hybrid Attacks

FENELLA BILLING* AND BIRGIT FELDTMANN**

Abstract

Hybrid threats have become a topic high on the international agenda. Hybrid threats and actual attacks may be classical criminal activities driven by personal motives and economic gain. However, this article deals with hybrid attacks that go beyond personally motivated criminal activity, aimed at states' vulnerabilities in a wider context. The hybrid nature of these attacks can engage different or hybrid legal responses – a criminal law response or an international law response to terrorism or a lead-up to armed conflict. The questions are, what is the role for criminal law in regulating hybrid attacks and what are the challenges of such an approach? Focusing on international and national criminal law regulating hybrid attacks, this article considers the three scenarios of attacks against critical infrastructure, jamming of maritime navigation and physical attacks on submarine cables and pipelines. The chapter highlights the complexities involved in criminal law approaches, requiring interaction and cooperation between the international and national levels, but also the potential advantages of integrating criminal law approaches into a broader military strategy.

* Fenella Billing is an Associate Professor of International Law and Human Rights, at the Department of Law, Faculty of Social Sciences and Humanities, Aalborg University, Denmark.

** Birgit Feldtmann is a Professor at the Department of Law, Faculty of Social Sciences and Humanities, Aalborg University, Denmark.

The ideas for this paper are based on a presentation to the Policing in a Digital Society Network conference held in Apeldoorn, Netherlands, from 15 to 17 November 2023 and the authors are grateful for the comments received on earlier drafts through the Network.

It is important to us to acknowledge the PDSN conference and network.

1. Introduction

Global interest in so-called 'hybrid threats' has developed into a topic high on the international agenda, having intensified in the past fifteen years, with Russia's 'distributed denial of service' cyberattacks on Estonia in 2007 as an early example.[1] Specific hybrid attacks have generated rapidly increasing concern, with the flat-out increase in dependence on computer systems, the interconnection of information and communication technology networks, and the increased mobilisation of people at all levels of modern society.[2] Incidents such as attacks against railway systems or the energy sector, the 'jamming' of navigational systems at sea, and the physical damaging of submarine pipelines or cables, illustrate the vulnerability of modern societies.[3] Some of these attacks might be 'classical' criminal activities driven by economic gain, such as the hacking of a computer system and paralysing it with malware, encrypting files and making them inaccessible, to obtain a ransom (so-called ransomware).[4] But such attacks can also go beyond mere criminal activity and be part of terrorist activities aimed at destabilising society, or connected to geopolitical interests of states and initiated or supported by states. Hybrid attacks can also be a part of hybrid warfare short of a full-blown armed conflict. This article deals with attacks in the modern society that go beyond mere criminal activity and are aimed at states' vulnerabilities in a wider context.[5] The hybrid nature of actual physical attacks and cyberattacks can engage different or hybrid legal responses. In absence of a clear and actual involvement in armed conflict, a criminal law response is the natural starting point. However, given the nature of hybrid attacks, states that are not at war may nevertheless claim a legal basis for regulation of these threats under the international law that applies in the lead up to war. This raises the question of what is the role of criminal law in relation to hybrid attacks?

Hybrid attacks are generally carried out in a grey zone between national and cross-border criminal activities, terrorism and/or warfare. This means that a criminal law approach to regulating these attacks faces particular legal complexities, as states maintain a legal grey zone between different legal concepts, categories and frameworks in criminal law, the international law supporting counterterrorism and the laws of war. Moreover, these different regulatory frameworks are co-existing at the international and national levels and can potentially operate concurrently. The underlying questions are, therefore, which regulatory frameworks are relevant, and how do they interrelate, when states deal with the incidents at hand in a criminal

1 Tikk, Kaska and Vihul (2010) pp. 14-35, Henderson (2024) p. 79.

2 Henderson (2024) p. 80, Akande, Coco and de Souza Dias (2021).

3 See Bach Jørgensen (2022), Moltke (2023), and Vock (2023), see further Fiott (2022) p. 11ff.

4 Milmo (2024).

5 See section 2 for a detailed explanation of what is meant in this article by the terms 'hybrid threats' and 'hybrid attacks'.

law setting; and what are the challenges connected to this approach? The aim of this contribution is to analyse the criminal law approach connected to hybrid attacks by taking three specific scenarios as examples. These scenarios are inspired by real events and include the hacking and disturbance of critical infrastructure, the 'jamming' of navigational systems at sea and the damaging of pipelines or cables on the seabed. While all these scenarios have been relevant for different European (and other) states, the perspective taken in this chapter examines attacks with a connection to Denmark, to include a specific national perspective in addition to the perspective of the international legal frameworks.

The article sets out with a brief introduction to the concept of hybrid threats (section 2). The article then delves into the criminal law approaches in three different scenarios inspired by recent events, by presenting the relevant international law, and introducing implementation at the national level, looking at the Danish law countering hybrid threats (sections 3-5). Based on sections 3-5, the article analyses the complexities of the legal settings and reflects on the challenges of using criminal law approaches to hybrid threats (section 6). The article finishes with some closing remarks (section 7).

2. The concept of hybrid attacks and legal implications

The concept of hybrid threats and attacks covers a diverse number of unwanted activities such as the 'weaponizing of migrants', cyberattacks against private or public systems, or physical attacks against critical infrastructure on land or at sea. Scholarship even discusses 'lawfare' as a hybrid threat in itself, whereby non-democratic states exploit legal uncertainty to maintain 'cold peace' scenarios.[6] Therefore, approaches against hybrid threats and specific attacks can also be diverse, may be taken on the national, regional and/or international levels, and include awareness, preventative and enforcement measures after an attack or attempted attack.

The issue of hybrid attacks is also a focal point of the European Union and 'has dominated the security landscape in Europe' in recent years.[7] While the term 'hybrid threats' is widely used in international and European debate, the concept of hybrid threats is not clearly defined or delimited in law. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) describes hybrid threats as activities that are:

> *planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. Such means include information manipulation, cyberattacks, economic influence or coercion, covert political manoeuvring, coercive diplomacy, or threats of military*

6 Siekiera (2023) pp. 109-112, Petrig (2024b) p. 88.

7 Giannopoulos, Smith and Theocharidou (2021) p. 4.

> *force. Hybrid threats describe a wide array of harmful activities with different goals, ranging from influence operations and interference all the way to hybrid warfare.*[8]

This means that 'hybrid threats' is a wide, complex and not clearly defined concept, including various possible acts committed with the intent to undermine state, institutional or organisational functions. The complexity of hybrid threats is further described in the following way:

> *Hybrid threats are diverse and ever-changing, and the tools used range from fake social media profiles to sophisticated cyber attacks, all the way to overt use of military force and everything in between. Hybrid influencing tools can be employed individually or in combination, depending on the nature of the target and the desired outcome. As a necessary consequence, countering hybrid threats must be an equally dynamic and adaptive activity, striving to keep abreast of variations of hybrid influencing and to predict where the emphasis will be next and which new tools may be employed.*[9]

A way to operationalise the concept of hybrid threats is presented by the Hybrid CoE which characterises hybrid threats in the following three ways:

> *1. Coordinated and synchronized action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means. 2. Activities that exploit the thresholds of detection and attribution, as well as the different interfaces (war-peace, internal-external security, local-state, and national-international). 3. Activities aimed at influencing different forms of decision-making at the local (regional), state, or institutional level, and designed to further and/or fulfil the agent's strategic goals while undermining and/or hurting the target.*[10]

In the context of this article, 'hybrid threats' are understood as encompassing the general danger (threat) of hybrid attacks, while the term 'hybrid attack' refers to specific coordinated action against private or public entities that deliberately target the systemic vulnerabilities of democratic states, institutions or private providers through a wide range of means with the aim of destabilisation. As briefly mentioned above and further demonstrated throughout this contribution, following this characterisation,

8 European Centre of Excellence for Countering Hybrid Threats.

9 Hagelstam (2018).

10 European Centre of Excellence for Countering Hybrid Threats, see also Henriksen (2015) pp. 330-331 and 333.

hybrid attacks are conducted in a grey zone between different legal concepts and different national, regional, and different frameworks of regulation. The interaction of hybrid attacks with other concepts can be illustrated in the following way:

Hybrid attacks can be targeted directly at states' functions and/or interests, but they can also be aimed at infrastructure, including infrastructure provided and manged by or provided to private entities, as well as state interests beyond borders. For example, attacks might be aimed at global positioning systems, pipelines or internet cables on the seabed, or interconnected electric systems, and therefore have widespread effects beyond the national level. This also means that a hybrid attack aiming at a national vulnerability might not only affect the targeted state, but also other states.[11] The complexity of hybrid attacks and possible counter-approaches also means that states may choose the legal categorisation of an attack according to the international relations aim in mind, for example, by choosing a warfare context that is more permissive of use of military force in response,[12] or by avoiding to categorise a specific hybrid attack in the scope of the *jus ad bellum* context and thereby downscaling specific incidents to be issues of terrorism and/or crime control. The following considerations deal with hybrid attacks from a criminal law approach and analyse multi-layered and multidimensional criminal law frameworks.

3. Attacks against critical infrastructure on land

3.1 Background to the problem – hacker attacks on critical infrastructure

Since the mid-1990s, the news of computer hacking has become more and more intense, requiring states to respond by enacting new laws against misuse of computers and the internet. Today, stories of attacks on critical infrastructure are one of the more common features of hybrid threats. Examples of cyberattacks with worldwide effects include: the Sony hack in 2014 by a group calling itself the 'Guardians of

11 Hagelstam (2018).

12 *E.g.* Petrig (2024b) pp. 89-90.

Peace', focusing on the release of the film 'The Interview' in which a North Korean ruler was assassinated, which destroyed computer systems and stole personal and commercial data, including unreleased movies;[13] and the SolarWinds attack in 2020, which 'penetrated the computer systems of thousands of organisations globally' but especially various parts of the United States government.[14] In Denmark, there are numerous recent examples. In November 2022, Danish DSB train services around the country stood still as a result of a hacker attack on the test environment for a security app, delivered by one firm to DSB.[15] In May 2023, a widespread and coordinated hacker attack was carried out against the Danish energy sector, affecting 22 energy and heating providers.[16] In forcing businesses to minimise damage by decoupling control of the services from the internet, some were forced to manage their services manually, including coordination with remote installations. It was reported that digital traces indicated that the hackers could have come from the Main Intelligence Directorate (GRU) of the Russian military's special services, Unit 74455 ('Sandworm').

3.2 The relevant international legal framework – the Budapest Convention 2001

While criminal hacker attacks may occur on the territory of one state, the perpetrators may be sitting in another state or utilising the server of another state. Therefore, an international harmonising framework can facilitate speedy and effective international criminal cooperation concerning hybrid threats, but it will always rely on criminal law operationalisation at the domestic level.

In November 2001, the Council of Europe's unique Convention on Cybercrime (Budapest Convention) was established to harmonise the criminal justice response to cybercrime and electronic evidence, both on land and at sea. In Section 1, on 'Substantive criminal law,' the State parties are obliged to adopt 'such legislative and other measures as may be necessary to establish [and sanction] as criminal offences under its domestic law' the offences set out in Articles 2-10, such as illegal access to a computer system, illegal interception of or interference with non-public transmissions of computer data and systems and misuse of devices, including attempted offences and offences committed by several accused acting with complicity. In Article 22, the Convention calls for State parties to establish prescriptive and enforcement jurisdiction over the offences if committed on the state's territory (territorial jurisdiction) or by a national against the law of the territory in which it was committed (active personality principle or nationality jurisdiction). The latter jurisdictional head would allow a state other than Denmark to prosecute hacker attacks committed in Denmark, particularly if Denmark has chosen not to prosecute, but to extradite the suspect to the State of

13 Henriksen (2015) p. 324.

14 Henderson (2024) pp. 79-80.

15 Slyngeborg Trolle (2022).

16 Moltke (2023).

nationality in accordance with the Convention's important obligation in cooperation on criminal matters to either extradite or prosecute offenders. Extradition would clearly rely on the receiving state having criminalised the same offending.

3.3 The relevant Danish criminal law

Whether or not criminal 'hackers' come from or act from a Budapest Convention state, the criminalisation of acts connected to hybrid threats, for example, the disruption of the train services, is fragmented on the Danish national level. The act of hacking is criminalised in Chapter 27 of the Danish Criminal Code dealing with violations of personal peace and reputation. Section 263(1) criminalises obtaining unlawful access to another person's (or company's) electronic data system. It is the mere accessing of another person's data system without their permission which is a violation of the provision, independent of whether this requires overcoming security measures (firewalls etc.). The provision also criminalises the abuse of a lawful access to the system, for example, if an employee is misusing a work-based access for other (unlawful) purposes.[17]

Attacks against critical infrastructure are further criminalised by several other specific provisions. For example, attacks against a railway system are criminalised in section 183, if they result in accidents. If an attack includes a threat to human life, severe damage or has the aim to destabilise society, it can be punished with life imprisonment (section 183(2)).[18] If the attack does not result in an accident, the mere interference with the safety of railway systems is criminalised in section 184.[19]

If dangerous acts like the above are conducted with terrorist intent,[20] for example, with the aim to seriously scare the population, unlawfully pressure public authorities or an international organisation, or to destabilise crucial societal structures, the acts would also fall under the criminalisation of terrorism in section 114 (and the following sections). This means that the concept of a terrorist act is defined by two main criteria: one is the specific intent, the other is that the act is explicitly mentioned in section 114, which includes acts falling under section 183, where such acts can cause serious damage to a country or international organisation.[21]

17 See Elholm *et al*. (2022) p. 582ff, Lentz (2024) p. 748 ff.

18 Elholm *et al.* (2022) p. 314 ff.

19 Elholm *et al.* (2022) p. 320 f.

20 See Grønning-Madsen (2023).

21 Elholm *et al.* (2022) p. 59 ff. On the requirement of the specific aim/motivation (*terrorismeforsæt*), see Grønning-Madsen (2023).

If a hacker attack against infrastructure fails or can be prevented by security measures, such as an effective firewall, it is punishable as an unlawful attempt of the above crimes according to section 21 of the Criminal Code. The concept of attempt in Danish criminal law is wide and includes any preparatory act as a step in the planned commitment of a crime.[22]

If a hacker attack is initiated outside of Denmark and aimed at infrastructure in Denmark, the act can be punished in Denmark (as the place where the harm occurs) under the principle of ubiquity, according to section 9(2) of the Criminal Code. Here the main question is whether the act has or was intended to have its effects in Denmark. This relates both to land territory and the territorial sea.[23]

3.4 Reflections on the interrelationship between the legal frameworks

Given that a Danish criminal law approach to hacking already presents with a panoply of provisions, hacker attacks on critical infrastructure illustrate well the value of harmonisation of criminal law at the international level. While there may be numerous potential offences in Denmark to cover a hacking attack, to secure some enforcement against such threats, double criminalisation of the same offences in two different countries makes it more difficult for suspects to escape investigations and prosecutions. Fitting with the global nature of hybrid threats, and in particular cyberattacks, for cooperation between signatory states, the Budapest Convention has certainly augmented the enforcement strength of criminal law, and its potential for prevention. Over the past 20 years, more than 125 states have adopted criminalisation laws, and more than 90 states have created investigative and prosecutorial powers in line with the treaty.[24] These numbers include numerous states from outside the Council of Europe, adding to the treaty's potential global impact despite it being a regional treaty.

4. Hybrid attacks against the safety and security of maritime navigation

4.1 Background to the problem - 'jamming' attacks of a ship's GPS signal

One way to attack a ship's safety and security is by jamming 'GPS' (Global Positioning System) signals. In October 2022, it was reported that the GPS navigational equipment on board four vessels became suddenly jammed for approximately 10 minutes, at the time when the pilots were about to navigate the Great Belt straight.[25] It was alleged that two Russian warships were identified approximately 20 kilometres away. Although the details of such episodes do not become matters of public knowledge, members

22 Langsted, Feldtmann and Lentz (2024) p. 209 ff.

23 Cornils and Greve (2014) p. 20 ff, Langsted, Feldtmann and Lentz (2024) p. 271.

24 Council of Europe (2022) p. 5.

25 Bach Jørgensen (2022).

of the Danish Defence Academy have commented that it is a known Russian modus operandi, to sow doubt and insecurity in the West about the capacity to protect people and critical infrastructure.[26]

4.2 The relevant international legal framework

4.2.1 The 2001 Budapest Convention

Using criminal law to counter jamming attacks against maritime navigation can also benefit from cooperation between Council of Europe states under the Budapest Convention. This again highlights the necessity for states' enactment of the duty to cooperate in Article 23, as well as the obligations under Article 22(1)(a) and (b), in relation to legislating for the creation of offences and procedures and, importantly, establishing jurisdiction over offences committed not only on the land territory of the state or by nationals of the state, but also in its territorial sea and over ships flying its flag.

4.2.2 The 1982 United Nations Convention on the Law of the Sea

When considering hybrid attacks occurring at sea, it may be relevant to consider the general prescriptive and enforcement jurisdiction established under the 1982 United Nations Convention on the Law of the Sea (UNCLOS), especially if a cyber-related incident involves a non-Budapest-signatory state or if the incident is non-cyber-related.

Under UNCLOS, law enforcement of hybrid attacks encountered at sea occurs in connection with the UNCLOS zonal system, setting out the geographical parameters for states' prescriptive and enforcement jurisdiction. The zonal system connects to the status of 'coastal states' and 'flag states', and to the respective and sometimes conflicting interests in use and management of the sea and marine resources. The main zones in connection with regulating hybrid attacks at sea are the territorial sea under the sovereignty of one state for 12 nautical miles from the coastal baseline; and the high seas, which do not come under the sovereignty of any one state but are part of what is understood as the global commons. The overlapping contiguous zone and exclusive economic zone (EEZ), giving coastal states certain rights in the high seas adjacent to the territorial sea, up to 24 and 200 nautical miles respectively, may also be relevant in a criminal law setting. In addition, provisions such as UNCLOS Article 88 reserve the use of the high seas for peaceful purposes.[27]

The rules about law enforcement jurisdiction at sea can thus be generally understood as reflecting three important principles: Firstly, the sovereignty of coastal states dominates the territorial seas, including the prescriptive and enforcement authority to regulate any crime that occurs within state sea-territory, as an extension of the same

26 Bach Jørgensen (2022).

27 Feldtmann (2023) p. 514 ff.

authority over crime occurring on land. UNCLOS Article 27 provides that a coastal state should not exercise its domestic criminal jurisdiction on board any ship engaged in 'innocent passage' through its territorial waters, yet it may do so under Article 27(2) to arrest a person or investigate a crime 'of the kind to disturb … the good order of the territorial sea'. Non-innocent passage in the territorial sea may involve research or surveyance, threatening or using force or, for example, cyber activities interfering with communication or positioning systems. Secondly, the principle of freedom of navigation limits coastal states' enforcement jurisdiction and ensures that all vessels may use all parts of the oceans, including territorial waters, if they are being used for innocent passage. Thirdly, freedom of the high seas reflects the high seas as a space without sovereignty; yet flag state jurisdiction under UNCLOS Article 92 creates an exclusive prescriptive and enforcement jurisdiction of a flag state over any incidents relevant to the criminal law occurring on the high seas on board ships flying that state's flag. Under Article 111 coastal states have a right to pursue a foreign vessel suspected of unlawful conduct beyond the territorial sea, but only if an uninterrupted 'hot pursuit' commences in the state's territorial sea. The combination of these principles creates a tension between the conflicting prescriptive and enforcement jurisdictions of coastal/port states and flag states, depending on where a vessel is located when malign conduct occurs. This can be added to by common principles for criminal law jurisdiction claimed by states over nationals who are accused of crime (the nationality or active personality principle) or nationals who are victims of crime (the passive personality principle).[28] This tension can be a central challenge in a criminal law approach.

In addition, in any maritime zone, if a cyber-attack can be interpreted as a 'use of force', then UNCLOS Article 301 can arguably apply, requiring states to refrain from 'any threat or use of force' against another state.[29] Under general international law, there is a debate about whether a cyber-attack on a state, by a another state, agents of a state or a (non-state) state-like entity, such as a terrorist group, can be considered a 'use of force', giving rise to a right of self-defence under the Charter of the United Nations Article 51. However, the legal parameters of the elements of the debate have not yet fully crystallised in state practice or international law (see also 6.3 below).

28 Crawford (2019) pp. 443-446.

29 Lohela and Schatz (2019) p. 19ff, see also UNCLOS Art 192, which may be relevant if a cyberattack also causes an oil spill or other form of marine pollution, and thereby violates the obligation to protect the marine environment; furthermore, the COLREGs may also be relevant insofar as they place a duty on vessels to conduct operations in such a way as to avoid collisions; cyberattacks on ships that then cause damage to ports, or cyberattacks directly aimed at port facilities also constitute internationally wrongful acts, against the sovereignty of other states: Schmitt (2017), Rule 4.

A further international treaty of specific relevance is the 2005 SUA Convention,[30] including the 1988 Convention for the Suppression of Unlawful Acts of Violence Against the Safety of Maritime Navigation and the 2005 Protocol (SUA Convention). Under Article 5, states are obliged to criminalise the offences in Article 3, including controlling another ship by use of force or intimidation, seriously interfering with the operation of a ship's navigational facilities in a way to endanger that ship's safe navigation, or attempting, assisting in or threatening to commit these crimes.[31] Article 4 provides that the SUA Convention does not apply when the victim ship is merely navigating in the territorial sea of a state, highlighting the importance of criminalisation of such offences in the coastal states' domestic law. Enforcement jurisdiction under the SUA Convention is relatively wide in Article 6, *requiring* (victim) flag state jurisdiction, territorial jurisdiction, including over offences occurring in the territorial sea, and jurisdiction according to the offender's nationality.[32] The Convention also *allows* additional heads of jurisdiction if the offending is committed by a stateless person, or involves a state's national being seized, threatened, injured or killed, or if the offence is (similar to terrorism) aimed at compelling the state establishing jurisdiction to do or abstain from doing any act.[33] Concerning general intelligence-sharing in international criminal law enforcement cooperation involving danger to human life at sea, the 1974 International Convention for the Safety of Life at Sea (SOLAS) may also become relevant.[34]

4.3 The relevant Danish criminal law

Interference with the navigation of a vessel (or other means of transportation) by means of 'unlawful pressure' is criminalised in section 183a of the Danish Criminal Code.[35] 'Unlawful pressure' (*ulovlig tvang*, according to section 260 of the Danish Criminal Code) is defined by the use of certain means of pressure, such as violence, threats of violence, or damage of goods, to force someone to do or refrain from doing something.[36] While the jamming of navigational systems can be understood as interference with the navigation of a vessel, and thus in the scope of section 183a,

30 Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (adopted 10 March 1988, entered into force 1 March 1992) and the 2005 Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (adopted 14 October 2005, entered into force 28 July 2010) (SUA Convention).

31 SUA Convention, Arts 3(1)(a), 3(1)(e) and 3(2).

32 SUA Convention, Arts 6(1)(a), (b) or (c).

33 SUA Convention, Arts 6(2)(a), (b) or (c).

34 International Convention for the Safety of Life at Sea (adopted 1 November 1974, entered into force 25 May 1980) (SOLAS Convention).

35 Elholm *et al.* (2022) p. 317 ff.

36 Elholm *et al.* (2022) p. 559 ff.

the inference is not obtained by the use of 'unlawful pressure' within the meaning of the provision. This means that the jamming of navigational systems surprisingly does not fall under the provision.

If the jamming results in an accident, it is criminalised under the above-mentioned section 183, which also criminalises the provocation of a maritime accident (*skibsbrud*), if it can be proved that the intention of the perpetrator is to cause damage to goods or injury to another person.[37] If the jamming does not result in an accident, the act would typically fall under the criminalisation in section 252, which criminalises, among other situations, recklessly creating a proximate danger (*nærliggende fare*) for human life or health.

Concerning jurisdiction, the main questions at stake at the time of the jamming are the location of the vessel, from which the jamming is initiated, and the location of navigation of the vessel, endangered by the jamming. This means that the issue of jurisdiction (or lack thereof) is influenced by the maritime zones set out in UNCLOS. If the jamming vessel is in Danish territorial water, the passage is not innocent and jurisdiction can be based on the territoriality principle in section 6, number 1 of the Criminal Code, consistent with the law of the sea. If the jamming affects vessels in Danish waters, the effects of the crime are in Denmark and jurisdiction is based on the principle of ubiquity in section 9(2).[38] However, due to the principle of exclusive jurisdiction of the flag state, Denmark could not exercise jurisdiction against a foreign-flagged vessel on the high seas without flag state consent.

4.4 Reflections on the interrelationship between the legal frameworks

Due to the global nature of cyberattacks on vessels at sea, the criminal law approach demands that states work together within international legal frameworks. Legal fragmentation at the international level, coupled with the operational necessity for criminalisation at a domestic level, can make enforcement jurisdiction at sea a complicated issue. While a criminal law approach in relation to jamming of a vessel's GPS signal may be simpler for signatory states cooperating under the Budapest Convention, even such a case can be made complicated by the matching of offences to achieve double criminalisation, when domestic criminal laws can appear as a patchwork of offences. The third and following example of a criminal law approach to hybrid threats presented in this study, falling outside the scope of the Budapest Convention, highlights this complicated yet intrinsic interrelationship between and within international and national law.

37 Elholm *et al.* (2022) p. 314 ff.

38 See part 3.3 above.

5. Hybrid attacks against pipelines and cables on the seabed

5.1 Background to the problem – the Nord Stream example

Around ninety-seven per cent of the world's internet data is transported through data cables at sea, and pipelines under water (and on land) are a crucial part of international supply systems carrying, for example, gas and oil.[39] This highlights the importance of such critical infrastructure across the globe and indicates the possible vulnerability of these structures. While pipelines and cables on land are usually set on state territory, and therefore protected by the legislation and the law enforcement agencies of the state, the situation is more complex when dealing with pipelines and cables on the seabed. This was clearly illustrated by the Nord Stream attacks in 2022 and most recently by the damaging of cables on the seabed of the Baltic Sea in November 2024.[40]

Taking the example of the Nord Stream incident: On 26 September 2022, several seismic explosions were recorded on the Nord Stream pipelines running from Russia to Germany in the Baltic Sea.[41] The pipelines were operated by Nord Stream AG and Nord Stream 2 AG, both majority-owned by Gazprom, a Russian state energy company. Data indicated that the first explosion to Nord Stream 2 occurred at 02:03:24 (CEST), located north-east of the Danish island of Bornholm, in the Danish EEZ. The second and third explosions were on Nord Stream 1, at 19:03:50 (CEST), in the Swedish EEZ, south of Dueodde. Seismic data reported by Norwegian researchers points to a fourth explosion south-west of Bornholm. Investigators confirmed that the pipelines were blasted with explosives.

In the immediate aftermath, the Danish Defence Force operated a no-fly, no-navigation zone around the leakages north-east of Bornholm, to protect the safety of air and sea traffic, enforced by a Danish warship, an environmental ship, and helicopters.[42] This force was later joined by a patrol ship. Sweden initiated similar measures in their EEZ.

The explosions were quickly placed into the context of the geopolitical situation with Russia's invasion of Ukraine,[43] and if proved they thus could be categorised as hybrid attacks. Several states, including Denmark, Sweden and Germany, but seemingly also Russia, initiated criminal investigations into the incident. It was initially reported in the media that Sweden, Denmark and Germany would establish a joint investigative team (JIT),[44] but this was rejected by Sweden with the argument that 'such a joint

39 Bafoutsou, Papaphilippou and Dekker (2023).

40 Government Offices of Sweden, Ministry of Defence (2024).

41 Bryant (2023), see also Swedish Security Services, Press room (2022), Nord Stream AG Press release (updated 14 November 2022).

42 Forsvaret (2022).

43 See *e.g.* Masih (2023).

44 On JIT's as a tool in international cooperation in criminal matters see Eurojust, Joint investigation teams. On the practice of JIT's see Furger (2024) p. 43 ff.

investigation would include legal agreements under which Sweden would have to share information from its own investigation that it deemed confidential.'[45]

In Denmark, the investigation engaged the national police (in Copenhagen), special services (PET) and energy providers.[46] The Danish investigation was formally terminated in mid-February 2024. The Copenhagen police issued a short press release stating that a complex and substantial investigation had been conducted and confirming that there had been acts of intentional sabotage.[47] Nevertheless, the police also concluded that there was no 'necessary basis for proceeding with a criminal case in Denmark'.[48] The specific legal basis for this conclusion remains unclear and no further explanation has been offered.

The Swedish investigation had already been terminated about two weeks before. In a press release, the Swedish prosecution service underlined that the investigation had been 'systematic and thorough' and had the aim 'to establish whether Swedish citizens were involved in the act and whether Swedish territory was used to carry out the act, and thereby risked damaging Swedish interests or Sweden's security.' The investigation was terminated with an explicit reference to the lack of Swedish criminal jurisdiction for the incidents, by concluding that 'Swedish jurisdiction does not apply and that the investigation therefore should be closed.'[49]

The German investigation is still on-going and in August 2024 the German authorities initiated a European Arrest Warrant for a Ukrainian citizen under the suspicion of involvement in the attacks against the Nord Stream pipelines.[50]

5.2 The relevant international legal framework

The issue of the protection of critical infrastructure on the seabed outside territorial waters and connected framework in international law is high on the international agenda. For example, in November 2024 the International Advisory Body for Submarine Cable Resilience was established by the International Telecommunication Union (ITU), the United Nations Agency for Digital Technologies and the International Cable Protection Committee (ICPC).[51] The aim of the Advisory Board is to 'address ways to improve cable resilience by promoting best practices for governments and industry players to ensure the timely deployment and repair of submarine cables,

45 More (2022).

46 Københavns Politi (2022).

47 Københavns Politi (2024).

48 Original text in the press release: 'Det er samtidig vurderingen, at der ikke er det fornødne grundlag for at forfølge en straffesag i Danmark' (own translation).

49 Åklagarmyndigheten (2024).

50 Bewarder *et al.* (2024).

51 International Advisory Body for Submarine Cable Resilience (2024).

reduce the risks of damage, and enhance the continuity of communications over the cables.'[52] While the prevention of damages to cables and pipelines on the seabed is a major priority, the question of the legal framework and in particular issues of prescriptive and enforcement jurisdiction are crucial questions been raised in the aftermath of the recent incidents, such as the Nord Stream incidents and the damage of cables in the Baltic Sea.

5.2.1. The regulation under the 1982 UNCLOS

As mentioned above (section 4), the legal regime at sea is created through the zonal system provided by the UNCLOS, setting out the geographical parameters for states' prescriptive and enforcement jurisdiction and securing rights and obligations for other states.

Concerning pipelines and cables in the territorial waters of the coastal state, similar to the situation on land, the starting point is that the territorial state has prescriptive and enforcement jurisdiction. At sea this is limited by the principle of innocent passage, but UNCLOS Article 21(1)(c) explicitly provides that the regulation of innocent passage by the coastal state includes protecting cables and pipelines. Therefore, wilful cable cuts and damage to pipelines in the territorial sea falls under the prescriptive and enforcement jurisdiction of a coastal state.

Outside territorial waters, UNCLOS Articles 58(1), 79(1) and 112 allow all states freedom to lay and maintain submarine cables and pipelines on the seabed in the EEZ and on the continental shelves of other states, as well as on the high seas.[53] The core of the EEZ-regime is that the coastal state, while it does not have general enforcement jurisdiction *per se,* has sovereign rights under Article 56 concerning the legitimate interests of exploration, exploitation, conservation and management of living and non-living resources in the water and on and below the seabed.[54] Coastal states also have exclusive rights and jurisdiction in the EEZ in relation to artificial islands and installations (Article 56 and 60), but not over transit cables or pipelines. Concerning other issues, such as the laying and maintenance of pipelines or cables and other *high seas freedoms* (in Article 87), the legal regime of the high seas also applies to the EEZ, creating a multilayered regulation. Under Article 58, when exercising high seas freedoms, states must respect the rights of, and laws adopted by coastal states in exercising control in the contiguous zone and EEZ.

Questions about criminal law jurisdiction in relation to submarine cables and pipelines may also be governed by general provisions of the UNCLOS, for example, concerning uninterrupted 'hot pursuit' of a vessel from territorial waters to the sea beyond.[55]

52 International Telecommunication Union (ITU) (2024).

53 Siig, Feldtmann and Billing (2024) p. 3 ff, see also UNCLOS arts 112 and 113.

54 See further *e.g*. UNCLOS Art 62.

55 *E.g*. UNCLOS Art 111.

Furthermore, wilful damage or damage by negligence of seabed cables and pipelines by a vessel in the high seas is subject to the exclusive jurisdiction of the flag state of the vessel causing the damage, pursuant to UNCLOS Articles 92 and 113. Article 113 also obliges states to have jurisdiction if the damage was caused 'by a person subject to its jurisdiction'. This means that a coastal state arguably does not even have the necessary power to fulfil the obligation to protect foreign submarine pipelines in its EEZ, as it only has the right to take reasonable measures for prevention, reduction and control of pollution from pipelines, and not a general right to ensure the safety of the pipeline from international shipping.[56]

5.2.2 Protection of submarine cables - 1884 Paris Convention

The 1884 Convention for the Protection of Submarine Telegraph Cables (Paris Convention) Article VIII provides for jurisdiction of the offending vessel's flag state in relation to 'infarctions' of the Convention. Alternatively, enforcement jurisdiction under general rules of criminal jurisdiction in domestic and international law falls to Convention states whose 'subjects and citizens' are involved. Proof of offences against submarine cables falls to the Convention states under Article X. However, the Article involves several grey areas, such as the scope of state powers to board a suspect vessel, the evidence-gathering qualifications of the officers involved, a lack of provision for fair trial rights in gathering evidence onboard, such as access to an interpreter, and the potential admissibility of any evidence gathered considering the procedural rights deficits.[57]

5.3 Relevant Danish criminal law

As with cyberattacks on critical infrastructure (see 3.3 above), physical attacks on internet and communication cables and pipelines on the seabed, for example by explosives, would fall under the criminalisation of terrorism in the Danish Criminal Code section 114 (and the following sections), if the necessary terrorism intent is present and the attacks fall within the serious crimes listed in the provision. One of the serious crimes mentioned in section 114 comes from section 193 of the Criminal Code. This provision criminalises, amongst other situations, a large-scale disruption of systems for the supply of energy and/or gas, as well as communication systems. This can be installations on land but also on the seabed. The means to obtain the disruption are not defined in the provision and, therefore, the serious disruption in itself forms the basis for criminal liability.[58]

56 SOLAS Convention, Chap. V, Rule 4 may also be relevant, requiring any Convention state that receives reliable intelligence of any dangers to notify anyone concerned and other interested governments.

57 See further Paige, Guilfoyle and McLaughlin (2020).

58 Elholm *et al*. (2020) p. 361 ff.

However, the use of some specific means to damage property, such as submarine cables and pipelines, is also criminalised. The initiation of an explosion with the intent to damage or destroy property is, together with other activities, specifically criminalised in section 183(1), and is also one of the offences included in the terrorism provisions (section 114 ff). Section 183(1) does not specify the type or severity of the explosion, but arguably it is only applicable to more serious explosions due to its severe punishment, with imprisonment of up to 12 years.[59]

If an attack against internet cables is conducted on land, the question of jurisdiction is answered on the basis of the principle of territoriality. Section 6, number 1, provides jurisdiction for all acts 'conducted in the Danish state',[60] meaning within Danish state territory.[61] This includes the Danish territorial sea. If the attack is conducted outside territorial waters, the situation gets more complex and the claim for jurisdiction is weak.

UNCLOS Article 56(1)(b)(i) provides coastal state jurisdiction in the EEZ concerning the establishment and use of artificial islands, installations and structures. The regulation of the EEZ by UNCLOS is supplemented on the national level by the Danish law on the continental shelf and certain activities in sea territory (*lov om kontinentalsoklen og visse aktiviteter på søterritorie*).[62] Section 3 of the Danish law also provides that Danish regulations are valid for 'installations exploring and exploiting resources' and their connected safety zones. However, transit cables and pipelines are not covered by this terminology, meaning that the Danish law is of limited application.

As mentioned above, UNCLOS Article 113 obliges states to have jurisdiction over a ship flying the state's flag or a person under its jurisdiction who is damaging a cable on the seabed. The Danish rules on jurisdiction include a general provision confirming criminal jurisdiction in situations where the act is regulated under international law; and section 8, number 5 of the Criminal Code obliges Denmark to establish this jurisdiction. In section 6, number 3, the Danish jurisdictional rules also include the flag state principle, meaning that there is Danish jurisdiction if a crime is committed on the high seas, onboard or from a Danish flagged vessel, including in the EEZ. Danish jurisdiction based on the active personality principle can also be linked to the perpetrator, if a Danish citizen or a person with residence in Denmark has committed an attack against cables on the seabed, in the EEZ or the high seas.[63] In particular, section 7(2) deals with acts committed outside the jurisdiction of another state.

59 Elholm *et al.* (2020) p. 314 ff.

60 In Danish 'i den danske stat', (own translation).

61 Langsted, Feldtmann and Lentz (2024) p. 270 f.

62 Bekendtgørelse af lov om kontinentalsoklen og visse aktiviteter på søterritorie, LBK nr.199 af 27.02.2024.

63 Cornils and Greve (2014) p. 23 ff.

If an attack against a transit cable/pipeline in the Danish EEZ is committed, the Danish regulations concerning protection of the environment can be engaged, if there is an environmental hazard.[64] But there is no general basis for regulation of and jurisdiction in situations where transit cables or pipelines are attacked. Those acts do not fall under the terminology 'in the Danish state' in section 6, number 1, and there is no specific provision dealing with this situation. It is also questionable whether a coastal state can exercise jurisdiction under the general regime in the law of the sea. The Swedish investigation of the Nord Stream 2 incident was explicitly terminated with the argument of lack of national jurisdiction,[65] and it is quite likely that the Danish closure of the case on the grounds that 'there is not the necessary basis for proceeding with a criminal case in Denmark' is also based on the lack of jurisdiction beyond the territorial sea.

5.4. Reflections on the interrelationship between the legal frameworks

The legal regulation of the EEZ in the law of the sea is complex, balancing different interests and creating overlapping legal regimes. This means that the distribution of possible criminal jurisdiction in connection with transit pipelines and cables is not comprehensive nor clearly regulated. Coastal states have jurisdiction and duties over various economic and conservation activities in the EEZ. However, despite the complex layers of regulation, the termination of the Danish and Swedish investigations into the Nord Stream incidents indicate that a lack of national jurisdiction to incidents occurring to cables and pipelines beyond the territorial sea is likely to be an obstacle for national criminal approaches, even when the incidents occur in the Danish EEZ and Denmark is one of the closest coastal states. Flag states and states of nationality have stronger claims to jurisdiction in such cases.

6. Assessing the challenges of a criminal law approach

6.1 International-national complexities

The three examples considered above illustrate the legal complexity when dealing with hybrid attacks in a criminal law context, particularly in the cases of globalised cyberattacks and extraterritorial attacks occurring at sea. Any questions of criminal law jurisdiction first relate directly to the domestic law and then indirectly to the ability of international frameworks to facilitate international cooperation. Thus, the examples demonstrate the need for international – national interaction to counteract some of the limitations of the criminal law.

The Danish examples also show that national regulation can be fragmented and present a myriad of potential offences. Denmark's approach towards creating offences

64 See UNCLOS Art. 56 (1)(b)(iii).

65 Kirby (2024).

relating to cyberattacks or hybrid attacks at sea has not been to initiate a comprehensive revision of the Criminal Code aimed at systematically dealing with cyberattacks, threats created through digital technology, the protection of digital infrastructure, nor attacks on critical infrastructure on the seabed. Instead, the different forms of hybrid attacks are dealt with in a complex mosaic of different criminalisations with different interests of protection. Most of the relevant provisions have been developed for analogous activities and do not specifically target digital behaviors or attacks at sea. While this tendency clearly creates a challenge, it may also lead to an overall comprehensiveness and thus a potential for adaptability in relation to prosecuting the different nuances of hybrid offending.

A major challenge leading from fragmented domestic criminalisation is the hurdle presented in relation to double criminalisation, which is commonly required as the hinge for international cooperation in law enforcement.[66] If two or more cooperating states all have overly complex or piecemeal criminalisation, then double criminalisation is more difficult to establish. Further, the domestic regulation of jurisdiction between the international and national Danish levels is fragmented and limited. For example, the principle of ubiquity (section 9(2), Danish Criminal Code) provides the basis for jurisdiction if a cyberattack affects systems in Denmark but also if the navigational systems of vessels in Danish territorial waters are jammed. Yet the execution of jurisdiction can be limited by the flag state principle. In other situations, such as attacks on underwater pipelines in the EEZ, there is simply no basis for the coastal state's jurisdiction.

On the international level, the regulation for setting enforcement jurisdiction, double criminalisation and investigative powers is also diverse and fragmented, dealing with various types of offending, including either specific offences, such as those in the Budapest Convention, or creating a general system of international cooperation or for upholding law and order at sea and providing rights and duties to states, as UNCLOS does.[67] The multilayered legal framework created by international law serves different purposes and interests. Moreover, as the example of cables and pipelines on the seabed shows, international law is not fully comprehensive and does not always have a clear division of rights and powers between states. Nevertheless, the more comprehensive approach to international cooperation based on harmonisation found in the Budapest Convention, makes for a clearer pathway to bringing global cyber-attackers to justice.

Nevertheless, while the path of a criminal law approach is not without its challenges, there are good reasons why states may still choose to deal with specific incidents within the criminal law framework. In the following, the questions of the role of criminal law and the challenges of a criminal law approach are further reflected upon.

66 See generally Boister (2023) pp. 218-257.

67 See Feldtmann (2024) p.11 ff.

6.2 The nature of criminal offending as part of potential hybrid 'warfare'

As a starting point to understanding the challenges and benefits of a criminal law approach to countering hybrid attacks, which occur on the background of nations in grey zones of potential conflict, it is necessary to unravel the relationship of the criminal and the potential enemy state. This has also been one of the hurdles to defining the crime of 'terrorism' more generally.[68] The complexity of the relationship emanates from various factors, including the fact that the offender could be acting on his or her own, or as part of a 'sub-national' group; it can be difficult to discern whether the motive is one of private or political ends; and the direct victims of the crime can be individuals and private enterprise within a state, rather than, or in addition to, the government agencies of a state. In the background, the legal concept of 'use of force' in war has also become increasingly difficult to define and attribution of responsibility for attacks to states has proved problematic.[69] While traditionally 'war' may have involved the use of military force between two or more states, and even could begin with a formal declaration of war, today, even the concept of war as a 'contest between states' has become blurred – distorted by the involvement of non-state actors as possible proxies and the use of hybrid means other than military force.

The difficulty of framing the perpetrator–state relationship in the case of hybrid attacks is exacerbated by the potential for such attacks to occur at the hands of state-backed non-state actors. For example, cyber-attackers can be 'hacktivists' acting alone, or they can be indirectly supported by a state through general funding and training, completely dependent on a state or effectively controlled by a state for a particular cyber operation and directly carrying out that state's instructions and/or directions.[70] The uncertainties and state centric legal approaches to warfare, confirm the benefits of operating within a law enforcement paradigm. This paradigm can help states avoid 'forcible responses' from enemy states for acts that may or may not be unlawful military force.[71]

6.3 The nature of hybrid attacks and the significance for counteroperations

As the three examples in this study highlight, a characteristic of hybrid attacks is the potential for broad effects, which result from the mere typing on a keyboard or from the actions of private individuals. Attacks on pipelines and cables at sea do not only affect vessels and people in the immediate vicinity but, as seen with the Nord Stream example, can affect an entire grid or the energy supply to an entire continent. Given the hidden, instantaneous, sweeping, global nature of the negative effects of

68 See *e.g.* Cantey (2023) p. 22 ff, Corn (2023) p. 223 f.

69 See *e.g.* Gray (2018) p. 136, on hybrid warfare and use of force at sea see generally Petrig (2024b).

70 See *Nicaragua v. United States of America*, 14, para 110 ff and 228.

71 Petrig (2024b) p. 89.

cyberattacks or physical attacks on critical infrastructure, the need for international cooperation with clear rules about enforcement jurisdiction is apparent, whether countermeasures in response come from within criminal law or the international law frameworks.[72]

The criminal law approach requires integrated operations, including action on national, regional and international levels; and an integrated national response, also termed 'Whole-of-society-approach'.[73] This integration calls for awareness and preparedness strategies, integrated with sufficient criminal law tools to counter cyber and other hybrid attacks and deal with the consequences when such attacks do occur. On the national level, the legal tools of a criminal law approach are primarily the creation of relevant offences and sufficient regulations of jurisdiction, as well as effective investigative powers and procedural rules to support efficient law enforcement.

Nevertheless, the actual investigation and/or enforcement of hybrid attacks will often be difficult in real life, as the perpetrator can be anywhere, and certain states may not be willing to cooperate. Furthermore, as with any form of terrorism, the difficulty of unravelling the cybercriminal from the state is heightened by the vagueness of domestic criminal law establishing the offence of terrorism. For example, as Ní Aoláin points out, the Human Rights Committee has expressed concern about the vagueness of the definition of terrorism in national criminal laws, using Article 114 of the Danish Criminal Code as an example.[74] Definition of hybrid attacks as criminal offences is, therefore, an area that requires considerable attention in the future, at the international/ regional and national levels.

Achieving sufficient levels of whole-of-society integration can be a challenge, and the examples above demonstrate that international/regional and national legal frameworks are only effective when they are intertwined and consistent. However, a criminal law approach can encourage states' authorities to plan and work together and align prevention and prosecution interests, rather than each state reacting in the heat of the moment out of purely national security interests.

6.4 The investigative challenges of the distance between the attacker and the attack

The stealth of cyberattacks and extraterritorial attacks at sea, and the difficulty to locate the origin of the cyber-related crime or extraterritorial crimes without eyewitnesses add complexity. For example, cyber risks result from the hostile activities of the attacker yet can be introduced into an entire organisation by unwitting employees or crew. The perpetrators could be on the other side of the world from the location of the effects of a cyber-attack or attack on seabed infrastructure. Victims are not

72 For a discussion of proportionate and necessary countermeasures in cyberspace under international law that do not involve use of (physical) force, see Henriksen (2015) pp. 342-350.

73 See Hagelstam (2018).

74 Ní Aoláin (2023) pp. 53-54.

necessarily territory-based and may instead be on a ship at sea. The physical isolation of ships, installations and submarine data cables and pipelines make them particularly vulnerable to physical and cyberattacks. Autonomous unmanned vessels (AUVs) may also be the target of a cyber-attack or be used as a perpetrator. [75]

A policing and law enforcement approach to hybrid attacks (as with terrorism generally) 'creates considerable pressure to provide evidence to a criminal justice system'.[76] Evidence gathering is the centerpiece to initiating criminal proceedings, and detaining and convicting suspects. Yet, the drive to obtain evidence of cyberattacks or attacks on pipelines is clearly a formidable challenge. On the other hand, this can be seen as one of the advantages of a criminal law approach of policing by agents who are equipped with focused, high-level investigative and forensic skills;[77] and, when international criminal cooperation is optimal, the police can cooperate with international colleagues to centralise the gathering of evidence.

6.5 The overall added value of a criminal law approach to hybrid threats contra warfare

Recently, it has been argued by individual states, states within the UN and in scholarship that a cyber-attack can be an unlawful use of force and, thereby, an act of aggression under the UN Charter Article 2(4), if committed by one state against another.[78] A similar argument can be applied to physical attacks against state-owned underwater pipelines. In discussion, states and scholars have referred to general rules and principles of international law and examples of 'voluntary, non-binding norms' in international instruments.[79] One issue is whether cyberattacks must involve physical harm to people or property, and what is the scale or gravity of the harm required to constitute a use of force, and thus place the attack within a laws of war paradigm.[80] Another question is whether it is possible for a series of cyberattacks to cumulatively constitute a use of force in a *jus ad bello* setting. The 'accumulation of events' doctrine has been accepted by some states, and is the position taken in the Tallinn Manuel 2.0.[81] Examples of cyberattacks cited in academic literature include cyberattacks carried out by Russia on Estonian energy networks in 2007, in its conflict with Georgia in 2008, and on Ukrainian power plants in 2015, and the USA and Israel's cyberattacks using a 'Stuxnet worm' against an Iranian nuclear plant in 2010.[82]

75 See Petrig (2024a).

76 Watkin (2023) p. 211.

77 See further Watkin (2023) p. 211.

78 Gray (2018) pp. 33-34 and 135, Hendersen (2024) p. 79 ff.

79 Akande *et al.* (2021), Hendersen (2024) p. 81ff.

80 Gray (2018) pp. 135-136, Hendersen (2024) pp. 96, 98 ff and 285 ff, Petrig (2024b) p. 88 ff.

81 Schmitt (2017) p. 342, Hendersen (2024) p. 294 f., Gray (2018) p. 136.

82 Gray (2018) pp. 33-34 and 261.

Indeed, a United Nations Group of Government Experts reported in 2021 that the UN Charter applies to cyber operations and arguably implied an 'inherent right' of states to take countermeasures in self-defence.[83] Thus, with its roots in the principles of distinction, proportionality and precaution,[84] yet another issue is whether a hybrid attack must be responded to with a qualitatively equivalent measure, or, for example, whether a state can justify responding to a cyber-attack with a conventional military response. Another problem is justifying the scale of a response in terms of civilians, geography and temporal scope.[85] Originating in such controversial fields of law, the questions of the applicability of the *jus ad bellum* and *jus in bello* rules and principles under international law to non-state actors, and to cyberattacks, point in the direction of the criminal law enforcement approach to regulating hybrid attacks. While acknowledging the advantages are generally more long term, Henriksen also discusses an alternative deescalating response of traditional methods of diplomatic and economic pressure and leverage.[86]

In relation to counterinsurgency and 'urban warfare', Watkins suggests that the needs to operate 'integrally "amongst the people"' and to return society back to normality 'point to the essential role policing performs … that transcends the conflict spectrum.'[87] The positioning of hybrid threats and cyberattacks within the arsenal of warfare creates a need for policing and criminal law frameworks to be integrated into a military strategy. Huntley and Regan discuss the benefits of a 'hybrid approach', akin to law enforcement, when countering threat networks, because 'dark networks' are often 'situated within a complex environment that contains many innocent individuals and legitimate social organizations.'[88] They add that non-lethal law enforcement measures such as surveillance, engagement with informants, arrest and property seizure allow for more individualised threat determinations and enhance the suppression of threat networks. These types of benefits can be transposed to countering dark networks in cyberspace or in connection with terrorism and emphasise the importance of policing in and amongst the innocent in today's world, even on the background of warfare, or potential warfare.

As an alternative to integrating criminal law and military responses, the approach of categorising specific hybrid or cyberattacks as crime rather than as a part of hybrid warfare is a way to downsize a potential conflict between states and deescalate. When the attacks against the Nord Stream pipelines became public knowledge, it was quite striking to observe that Denmark clearly was labelling the attacks in a criminal law

83 Hendersen (2024) p. 271.

84 See *e.g.* Petrig (2024b) p. 99 f.

85 Hendersen (2024) p. 318 ff.

86 Henriksen (2015) p. 328.

87 Watkin (2023) p. 235 f.

88 Huntley and Regan (2023) pp. 461-462.

context, avoiding an explicit, formal link of the incident to Russia's on-going war in Ukraine. This means that the criminal law approach might serve a purpose, even if it does not ultimately result in the conviction of an offender.

7. Conclusions - What is the role of criminal law?

Legal jurisdiction to enforce criminal law approaches under the international law instruments, such as the 2001 Budapest Convention Article 22(4), or the 2005 SUA Convention Article 6, does not and cannot exclude the criminal law jurisdiction of the cooperating states under domestic law. Likewise, effectively suppressing and fighting cybercrime or attacks on infrastructure at sea under domestic law, by its nature, requires a greater level of international cooperation. To overcome the mosaic of domestic criminal laws that hinder double criminalisation, more international consensus is needed in relation to criminalising hybrid attacks. Moreover, an increased effort towards international legal frameworks is required to enhance multilevel clarification of jurisdiction, harmonised criminalisation and to facilitate adaptable, international cooperation in criminal law enforcement by nation states, a purpose that is perhaps most successfully achieved today within the framework of the Budapest Convention.

In addition, detecting, suppressing, investigating and prosecuting crime requires a dynamic integrated legal response that coordinates and empowers cooperation between various state authorities and other parts of society. As demonstrated in this study, a criminal law approach to fighting hybrid attacks is a complex matter of integrating disparate states' interests in creating a global net of prevention strategies with enforcement jurisdiction and prosecutorial reach.

Modern warfare seems to rely more heavily on transnational criminal activity, including cyberattacks on non-combatants by non-combatants, and therefore, despite the challenges, a law enforcement approach to hybrid threats is an unavoidable imperative, even when perceived as part of a larger military operation. The question for the future is how criminal law can facilitate policing and gathering evidence of hybrid attacks in the most effective way, while bearing in mind the human rights of victims, the need for fairness to a suspect or accused, and the need to preserve the crimes' innocent surroundings in global society, rather than harming the innocent at the same time.

Reference list

Treaties

Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation (adopted 10 March 19888 and entered into force 1 March 1992).

Convention on International Regulations for Preventing Collisions at Sea (adopted 20 October 1972 and entered into force 15 July 1977) (COLREGs).

Council of Europe, Convention on Cybercrime 2001 (adopted 23 November 2001 and entered into force 1 July 2004) ETS No. 185 (Budapest Convention).

International Convention for the Safety of Life at Sea (adopted 1 November 1974, entered into force 25 May 1980) (SOLAS).

Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf (adopted 14 October 2005 and entered into force 28 July 2010) (SUA Convention).

United Nations Convention on the Law of the Sea 1982 (opened for signature 10 December 1982, entered into force 14 November 1994) (UNCLOS).

Legislation

LBK nr.199 af 27.02.2024 Bekendtgørelse af lov om kontinentalsoklen og visse aktiviteter på søterritorie.

Case law

Case concerning military and paramilitary activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986.

Books and Reports

Bafoutsou G, Papaphilippou M and Dekker M (2023) *Subsea Cables – What is at Stake?* ENISA Publications, Office of the European Union. Available from: (URL). Accessed 28 October 2024.

Council of Europe (2022) *Convention on Cybercrime: Special edition dedicated to the drafters of the Convention (1997-2001)*. Strasbourg: Council of Europe. Available from: (URL). Accessed 28 October 2024.

Crawford J (2019) *Brownlie's Principles of Public International Law* 9th edition. Oxford University Press.

Elholm T, *et al.* (2022) *Kommenteret Straffelov, Almindelig del* 12th edn. DJØF Forlag.

Fiott D (2022) *Hybrid CoE Paper 13 Digitalization and hybrid threats: Assessing the vulnerabilities for European security.* The European Centre of Excellence for Countering Hybrid Threats. Available from: (URL).

Giannopoulos G, Smith H and Theocharidou M (eds.) (2021) *The Landscape of Hybrid Threats: A Conceptual Model.* Publications Office of the European Union. Available from: (URL).

Gray C (2018) *International Law and the Use of Force* 4th edition. Oxford University Press.

Grønning-Madsen N (2023) *Terrorismeforsættet – En Analyse af Straffelovens §114*. Karnov Group.

Hagelstam A (2018) *Cooperating to counter hybrid threats.* NATO. Available from: (URL). Accessed on 19 February 2024.

Henderson C (2024) *The Use of Force and International Law (2nd edition)*. Cambridge University Press.

Langsted L B, Feldtmann B and Lentz L W (2024) *Waabens Strafferettens, Almindelig del* 7th edition. Karnov.

Lohela T and Schatz V (eds.) (2019) *Hybrid CoE Working Paper 5 Handbook on Maritime Hybrid Threats – 10 Scenarios and legal scans*. The European Centre of Excellence for Countering Hybrid Threats. Available from: (URL). Accessed on 19 February 2024.

Schmitt M N (ed.) (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

Tikk E, Kaska K and Vihul L (2010) *International Cyber Incidents: Legal Considerations*. Cooperative Cyber Defence Center of Excellence (CCD COE). Available from: (URL). Accessed 28 October 2024.

Articles and book chapters

Boister N (2023) A History of Double Criminality in Extradition. *Journal of the History of International Law* 25, 218-257.

Cantey S (2023) Non-State Actors, Terrorism, and the War Paradigm Revisited, in eds. Finkelstein C, *et al. Between Crime and War: Hybrid Legal Frameworks for Asymmetric Conflict.* Oxford University Press, 21-43.

Corn G S (2023) Ratchet Down or Ramp Up? Contemporary Threats, Armed Conflict, and Tailored Authority, in eds. Finkelstein C, *et al. Between Crime and War: Hybrid Legal Frameworks for Asymmetric Conflict.* Oxford University Press, 223-264.

Cornils K and Greve V (2014) Chapter 1: Denmark, in eds. Elholm T and Feldtmann B *Criminal Jurisdiction: A Nordic Perspective.* DJØF Forlag, 11-35.

Feldtmann B (2023) Den internationale havret, in eds. Harhoff F and Daniel B T *Folkeret* 2nd edition. Han Reitzels Forlag, 513-565.

Feldtmann B (2024) The System of Law and Order at Sea Under UNCLOS 1982, in eds. Siig K, Feldtmann B and Billing F M W *United Nations Convention on the Law of the Sea: A System of Regulation.* Routledge,11-24.

Furger A (2024) Can They Deliver? The Practice of Joint Investigation Teams (JITS). *Core International Crimes Investigations, Journal of International Criminal Justice* 22 (1), 43-58.

Henriksen A (2015) Lawful State Responses to Low-Level Cyber-attacks. *Nordic Journal of International Law* 84, 323-351.

Huntley T and Regan M (2023) From Armed Conflict to Countering Threat Networks: Counterterrorism and Social Network Analysis, in eds Finkelstein C, *et al. Between Crime and War: Hybrid Legal Frameworks for Asymmetric Conflict.* Oxford University Press, 437-470.

Lentz L W (2024) Cybercrime og politiets efterforskning, in ed. Trzaskowski J *Internetretten* 4th edition. Ex Tuto, 737-774.

Ní Aoláin F (2023) The Limits of Law and the Value of Rights in Addressing Terrorism, in eds. Finkelstein C, *et al. Between Crime and War: Hybrid Legal Frameworks for Asymmetric Conflict.* Oxford University Press, 45-62.

Petrig A (2024a) Unmanned Vessels and the Multi-dimensional Concept of 'Ship' Under UNCLOS 1982, in eds. Siig K, Feldtmann B and Billing F M W *United Nations Convention on the Law of the Sea: A System of Regulation*. Routledge, 45-62.

Petrig A (2024b) Use of Force in Hybrid Naval Warfare Contexts: Applicability of the Law Enforcement or Conduct of Hostilities Rules?, in ed. Lott A *Maritime Security Law in Hybrid Warfare.* Brill Nijhoff, 86-121.

Siekiera J (2023) International legal framework regulating military exercises – Lawfare potentially associated with military exercises as a hybrid threat. *International Law Quarterly* 1(1), 107-125.

Siig K, Feldtmann B and Billing F M W (2024) Introduction to UNCLOS 1982 as a System of Regulation, in eds. Siig K, Feldtmann B and Billing F M W *United Nations Convention on the Law of the Sea: A System of Regulation*. Routledge, 1-8.

Watkin K (2023) Urban Warfare: Policing Conflict, in eds. Finkelstein C *et al. Between Crime and War: Hybrid Legal Frameworks for Asymmetric Conflict.* Oxford University Press, 183-221.

Blogs

Akande D, Coco A and de Souza Dias T (2021) Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond. *EJIL: Talk!*. Available from: (URL). Accessed on 19 February 2024.

Paige T P, Guilfoyle D and McLaughlin R (2020) The Final Frontier of Cyberspace: Ensuring that Submarine Data Cables are Able to Live Long and Prosper (Part I and Part II). *Opinio Juris*. Available from: (URL). Accessed on 19 February 2024.

Newspaper articles

Bach Jørgensen L (2022) *Russiske krigsskibe kan have leget kispus med danske lodser*. TV2 Nyheder. Available from: (URL). Accessed on 19 September 2024.

Bewarder M, *et al.* (2024) *Erster Haftbefehl wegen Nord-Stream-Anschlägen*. Tagesschau. Available from: (URL). Accessed on 19 September 2024.

Bryant M (2023) *Key details behind Nord Stream pipeline blasts revealed by scientists - Researchers in Norway reveal further analysis of 2022 explosions as well as a detailed timeline of events*. The Guardian. Available from: (URL). Accessed on 19 February 2024.

Kirby P (2024) *Sweden Shuts Down Nord Stream Blast Inquiry*. BBC news. Available from: (URL). Accessed on 19 September 2024.

Masih N (2023) *Who blew up the Nord Stream pipelines? What we know one year later*. Washinton Post. Available from: (URL). Accessed on 19 September 2024.

Milmo D (2024) *Cyber-hacking victims'paid out record $1.1bn in ransoms last year': Ransomware gangs targeted hospitals, schools and bodies such as BA and the BBC, Chainalysis finds*. The Guardian. Available from: (URL). Accessed on 19 February 2024.

Moltke H (2023) *Energisektorenramt af det 'hidtil mest omfangsrige' cyberangreb.* Danmarks Radio. Available from: (URL). Accessed on 19 September 2024.

More R (2022) *Sweden shuns formal joint investigation of Nord Stream leak, citing national security*. Reuters. Available from: (URL). Accessed on 19 September 2024.

Slyngeborg Trolle J (2022) *DSB: Lørdagens totalnedbrud af togdriften skyldtes hackerangreb og fejl i nødprocedure.* Danmarks Radio. Available from: (URL). Accessed on 19 February 2024.

Vock I (2023) *Sweden investigating damage to Baltic undersea cable*. BBC News. Available from: (URL). Accessed on 19 September 2024.

Press Release

Forsvaret (2022) *Gaslækage i Østersøen: Efter de tre gaslækager på Nord Stream-gasledningerne i Østersøen har Forsvaret indsat fregatten Absalon og miljøskibet Gunnar Thorson smat en helikopterkapacitet.* Forsvaret. Available from: (URL).

Government Offices of Sweden; Ministry of Defence (2024) *Statement regarding damaged communications cable by the Swedish and Lithuanian ministers for defence*. Available from: (URL). Accessed on 3 December 2024.

International Telecommunication Union (ITU) (2024) *Launch of international advisory body to support resilience of submarine telecom cables*. Available from: (URL). Accessed on 3 December 2024.

Københavns Politi (2022) *Status på efterforskningen af gaslækagerne i Østersøen*. Københavns Politi Nyhed. Available from (URL). Accessed on 30 April 2024.

Københavns Politi (2024) *Københavns Politi og PET's fælles efterforskning af sprængningerne af Nord Stream indstilles.* Københavns Politi Nyhed. Available from: (URL). Accessed on 30 April 2024.

Nord Stream AG (2022) *Incident on the Nord Stream Pipeline (updated 14/11/2022)*. Press hotline, Switzerland. Available from (URL). Accessed on 19 February 2024.

Swedish Security Services (2022) *Strengthened suspicions of gross sabotage in Baltic Sea. Press room.* Available from (URL). Accessed on 19 February 2024.

Åklagarmyndigheten (2024) *The prosecutor closes the Swedish investigation concerning gross sabotage against Nord Stream*. Available from (URL). Accessed on 19 September 2024.

Websites

Eurojust *Joint Investigative Teams.* Available from (URL). Accessed on 19 September 2024.

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE). *Hybrid threats as a concept*. Available from: (URL). Accessed on 19 February 2024.

International Advisory Body for Submarine Cable Resilience. Available form: (URL). Accessed on 3 December 2024.