Countering cyberterrorism

Candidate 6017

Word count: 3599

Table of content

1. Introduction

History has over the years illustrated the diversity in methods and operational tactics of terrorism. Now, the emergence of cyberterrorism represents a new challenge compared to the earliest cases when the *Sicariis* [1] attacked their victims with knifes in public spaces to ISIS using vehicles along the beach side in Nice, France (Nacos, 2019, p. 45; Sassard, 2016). Terrorism has caused many changes around the world, and the tactic has sparked much fear and controversies. It has led to the destabilization of regimes and other political, economic, social, and cultural environments (Nacos, 2019). Today the concept is yet to have a clear definition and governments lack the appropriate understanding of how they best can counter this ever-evolving phenomenon. Henceforth, this assignment aims to illuminate why terrorism, and cyberterrorism can be described as 'wicked problems' and discuss how such problems can be countered.

1.2 Structure

This paper is divided into four parts. First, the introduction and review of relevant theoretical literature. Secondly, follows a discussion on *terrorism* and *wicked problems* as concepts. Afterwards, the paper addresses some challenges and advantages related to regulating wicked problems using a risk-based regime with Norway as an example. Third, the paper will describe what cyberterrorism is and why a clear understanding is important for societies to become resilient against it. Lastly, I argue that a combination of risk-based regime and the rule-compliance regime may be a reasonable solution when building societies that are resilient to cyberterrorism.

1.3 Theoretical framework and concepts

This section will shortly introduce the concepts of security, resilience, and wicked problems. Later, these concepts will be discussed in light of the concepts of terrorism and cyberterrorism.

As demarcated by Jore, terrorism is a wicked security problem and not safety (Almklov et al., 2018, p. 1; Jore, 2019a, p. 150). This focus may be due to the possible overlap between the definition of security and terrorism. Hereafter, security is defined as:

[1] Sicariis could be considered a terror group that were involved with the Zealots' fight against Roman occupiers of Palestine. They killed their victims in the name of God, often with a political motive. Their targets where often found in large spaces on holidays. Their terror campaign ended AD 73 (Nacos, 2019, p. 45).

> "…the perceived or actual ability to prepare for, adapt to, withstand, and recover from dangers and crisis caused by people's deliberate, intentional, and malicious acts such as terrorism, sabotage, organized crime, or hacking." (Jore, 2019b, p. 157)

The *ability to prepare for, adapt to, withstand, and recover* are also essential elements of a resilient society (Almklov et al., 2018). Consequently, the understanding of terrorism as a problem, as well as cyberterrorism, affects how countries like Norway develop counterterrorism measures and build their resilient societies against such threats.

In order to answer the assignment Fischbacher-Smith's (2016) discussion on the United Kingdom counterterrorism policies gives a firm basis in understanding why terrorism can be considered a wicked problem (Fischbacher-Smith, 2016, p. 402). The arguments he presents can also be considered when evaluating cyberterrorism as a wicked problem. His work can also be related to problems identified by Jore, concerning the standardization of terrorism risk analysis, and the construction of resilient societies (2019b; 2015). Therefore, we can assess whether a risk-based regime is indeed the best way to build a resilient society. This paper argues that whether such a regime is appropriate to counter terrorism or not we must understand what it is, and why it may be considered a wicked problem.

2. Terrorism as a wicked problem

Normally we include a definition of what terrorism is in order to understand how to counter it, but this is where the challenges start. The ambiguity of what constitutes as terrorism, the related uncertainty and lack of a clear and unitary definition reduces governments and security agencies ability to counter it. As they do not have a common understanding of what terrorism is, it affects which counterterrorism measures they implement, and their efficiency. The same goes for the standardization of terrorism management (Fischbacher-Smith, 2016, p. 403; Jore, 2019a, 2019d).

This paper considers terrorism as an umbrella term, as it encompasses many forms of the phenomenon, such as cyberterrorism. This results in divergent understandings or perceptions of the problem and is one of the key points in categorizing terrorism as a wicked problem. As Fischbacher-Smith points out:

> "What makes terrorism such a wicked policy problem is the diversity that is present within the various attack vectors that are available to them (and the associated intensity of those attacks); the potential range of targets that are open to being attacked; and the potential force multipliers that can be found within the

> urban and organizational spaces in which they choose to mount their attack." (Fischbacher-Smith, 2016, p. 400)

Breaking it down, terrorism is so complex and highly unpredictable in its nature which in turn makes it extremely difficult to handle. We do not know when, where, how, or who is carrying out the next attack. Whether it will be a 'lone wolf'-attack on a mosque such as the Manshaus-case in Bærum, 2019 (Dalgaard-Nilsen et al., 2020)? Or for example a cyberattack against infrastructures such as Stuxnet in 2010 and NotPetya in 2017 (Langner, 2011; McQuade, 2018). Or perhaps a chemical, biological, radiological or nuclear (CBRN) attack, as we saw in Tokyo, 1995 (Ivanova & Sandler, 2007). The uncertainty related to the diversity in methods, targets and actors reduces our ability to develop counterterrorism measures that work efficiently (Jore, 2019d).

Additionally, as the concept is not neutral, the side effects of defining someone as a terrorist, or a terrorist group have significant consequences. This is because terrorism often relates to two characteristics: 1) the motives are political, and 2) the targets are civilians or non-combatants (Nacos, 2015). These factors are important to have in mind as the meaning we apply to terrorism and its perpetrators is guiding for how we shape everything from judicial frameworks to the counterterrorism measures. Nevertheless, this paper will use the definition by Weinberg, Pedahzur and Hirsch-Hoefler (2004) so the reader may have clearer understanding of the paper's interpretation. Terrorism is then recognized as:

> "… a politically motivated tactic involving the threat or use of force or violence in which the pursuit of publicity plays a significant role." (Weinberg et al., 2004, p. 786)

The definition may be criticised for being too broad, yet it serves the purpose of this paper by being short and precise and entails the two aspects mentioned by Nacos (2015). Besides, it can easily be related to the definition of cyberterrorism that will be presented later.

2.1 Does a risk-based regulatory regime work on wicked problems?

First, regulatory regimes can be understood as strategies that are applied to counter wicked problems such as terrorism. Therefore, it is important to have in mind that it is often difficult to assess whether implemented measures or strategies truly work. As security is a non-event it is hard to measure the effectiveness of countermeasures (Jore, 2019a, p. 7). However, I will attempt to evaluate whether the regimes work by assessing related challenges and advantages.

For instance, one of the main challenges for the risk-based regime is that it is particularly reliant on trust. As Jore (2015) points out,

> "Such a regime is based upon a belief about the regulated wanting and pursuing the best solutions available." (Jore, 2015, p. 6).

As a result, this belief affects how the management relationship within risk-based regulatory regimes are formed. Take Norway as an example, here several businesses in charge of critical infrastructures are legally bounded by the National Security Act (NSA) 2019. The NSA is an example of the Norwegian government's risk-based regulatory regime. Here businesses that are required to follow the law are obligated to conduct risk assessments and implement security measures to reduce risks they identify (Jore, 2019c, 2019d; Justis- og beredskapsdepartementet, 2019). Unfortunately, the thoroughness of these assessments and the following implementation of security measures vary, as several industries have to balance cost and benefits differently (Jore, 2019d). Therefore, seeing that wicked problems often are difficult to define and assess the probability and possible consequences of this in turn may lower some businesses willingness to reduce the risk connected to such problems. Consequently, we need to ask whether a shift towards such a trust reliant regime is suitable when we shall counter transboundary wicked problems.

On the other hand, the flexibility that the risk-based regime provides is one of its main advantages. For example, bearing in mind the enormous development within the information and communications technology (ICT) the past decades, the threat landscape in cyber space changes every day. The implementation of one rule today may cause the development of new methods and targets tomorrow. Thus, assuming we consider cyberterrorism a wicked problem it is essential to understand that the digital environment is constantly changing (NSM, 2020). Therefore, by giving organizations more flexibility they can implement security measures that fit their needs, and the changing environment. By requiring businesses to conduct risk assessments and implement measures accordingly they become better secured when meeting new changes within the threat landscape. This would probably not be as easy in a rule-compliance regime where businesses must strictly follow certain, static rules. Yet, trust is still an important factor that represent a vulnerability that may need stringent management.

As the risk-based regime does not provide any guide on how to construct good security, businesses may find themselves not knowing what measures to implement, where, why, and how (Jore, 2015). Therefore, a combination with the rule-compliance regime may be necessary.

Rules can then serve as minimum standards that businesses need to follow, and when their security needs improvement it is their responsibility. Such a proposal may result in businesses thinking that the rules implemented by the government are good enough. However, it is important to remember that minimum standards do not guarantee security. If rules are in focus it may direct companies' security efforts in a wrong direction.

As priorities differ it is important to understand that different sectors have different threats, values, and vulnerabilities. Rule-compliance regimes tend to be uniform and somewhat static, meaning rules are set equally for different organizations and not continuously updated according to the threat picture (Jore, 2015, p. 3). Risk-based regulatory regimes will, on the other hand, be more dynamic as it focuses on the function that businesses need to be uphold.

If we want to steer an organization's attention in the right direction, we should focus on the everchanging threat landscape. A risk-based regime may be the solution as relevant actors are forced to consider the environment that surrounds them and evaluate and update their security accordingly. Take the Norwegian company *Lyse* as an example. Lyse oversees several power plants and need to have a certain level of security (Lyse Konsern, 2020). Let us say that their digital fire walls require a certain level of security which is set according to their installation's criticality. The degree of security then varies according to the assessment of how critical their power plant is, depending upon the assessment done by themselves. The government can then supervise what security measures are implemented and evaluate if it is according to the installations level of criticality.

In short, the nature of wicked problems requires a multidisciplinary approach. As Hopkins (2011) argues, the regimes are complimentary and not mutually exclusive. By solely applying a risk-based regime we may not be able to reduce all necessary risks. Owing the multifaceted and transboundary characteristics of wicked problems we could argue that a combination of the two regimes could be an appropriate combination to counter cyberterrorism (Jore, 2015, Jore, 2019d). How such a regime would and should look like then depends on what cyberterrorism is and how it works.

3. How to build a resilient society against cyberterrorism

When building resilient societies, we should focus on making them safer. This suggests a reduction of risks related to the society that needs to build its resilience and an involvement of relevant actors (Almklov et al., 2018). How we reduce risks can be done in many ways. In this

section we will evaluate what type of regulatory regime is the best to counter cyberterrorism. Reducing risks is then understood as a way of countering something, such as cyberterrorism.

One way to strengthen societies resilience is by developing regulatory regimes that make actors in charge of a societal safety and security, responsible for their activities. Consequently, they need to know what to prevent and how to prevent it. This implies the need for a common understanding of what measures are the most effective. Our primary focus should then be to understand what cyberterrorism is and how it can affect us.

If we understand the word *cyber* as a prefix, its combination with the word *terrorism* limits the research paper to the digital part of terrorism. This gives us some of the same challenges that are apparent when trying to counter terrorism. However, by concentrating on how to counter cyberterrorism we limit ourselves to focus only on those terrorists, groups and attacks that are related to the digital environment.

Such an approach may be criticized by experts as Richard Clarke. He means the words 'cyber' and 'terrorism' should not be conjugated because it gives us a misleading understanding of what it is. Clarke argues that people then would be likely to "… conjure images of bin Laden waging cyber war from his cave." (Clarke & Knake, 2014, p. 66) Even though I understand the argument, the assessment is inadequate as I believe cyberterrorism is not necessarily waged only by groups such as Al-Qaeda or ISIS. For example, as the Cyberspace Policy Review (2010) states: "… A growing array of state and non-state actors such as terrorist and international criminal groups are targeting U.S. citizens, commerce, critical infrastructure, and government." (Nacos, 2019, p. 356). This suggests that state actors can also be considered cyberterrorists.

Moreover, in a lecture at the University of Stavanger, Tegg Westbrook raises the question of what a digital risk is, if cyberterrorism really exists, and who can be considered a cyberterrorist. Westbrook points out that there are many grey zone actions and activities that may be tagged with the labels 'cyber' and 'terror' (Westbrook T., personal communication, 14.09.2020). Again, this definitional issue requires attention as our understanding of who can be considered a cyberterrorist, and what constitutes as cyberterrorism affects how a regulatory regime shall look like. Thus, cyberterrorism will be understood according to Theohary and Rollins (2015) as:

> "… the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." (Theohary & Rollins, 2015, p. 1).

A cyberterrorist is then considered as: "… state-sponsored and non-state actors who engage in cyberattacks to pursue their objectives." (Theohary & Rollins, 2015, p. 2) The first definition should be seen in relation to Weinberg, Pedahzur and Hirsch-Hoefler's (2004) definition of terrorism and our understanding of wicked problems. The reader should also be aware of the definitions limitations as it does not address what constitutes as *disruptive activities* and that it limits itself to activities against computers/and or networks.

Cyberspace is gradually becoming a more attractive battleground, and digital tools are more utilized. Disruptive activities are then understood as *all* types of actions conducted over, or with the use of digital tools to cause harm, or the threat thereof. As a result, I would argue for a definition that also includes attacks against physical infrastructures, peoples, and groups. This is because we over the last decades have seen how digital tools can be utilized to create physical destruction and psychological harm and manipulation (Nacos, 2019, p. 361). Some examples of physical destruction is the Aurora Generator Test in 2007, the remote controlling of a tram in Podz, Poland 2008, Stuxnet cyberattack in 2010 and the hack on the Ukrainian power grid in 2015 (Zeller, 2011; Vilhelm, 2015; Langner, 2011; CISA, 2016; Zetter, 2016). These are not defined as acts of cyberterrorism but illustrate the potential it might have. Defining cyberterrorism as disruptive activities might then be misleading as it understates the damage potential.

3.1 A risk-based, and rule-compliant regulatory regime

As argued in chapter 4, wicked problems such as cyberterrorism, cannot solely be met by a risk-based regulatory regime. It needs to be combined with the rule-compliance regime as constant discoveries and developments of new innovations create new digital risks. All apps, programs, codes, and other digital tools and devices comes with vulnerabilities that can be exploited by the 'calculated aggressor' (Jore, 2015; Jore, 2019c, p. 9). Similarly, as we are becoming more connected to the internet, we are also more susceptible for cyberattacks.

Therefore, when constructing a resilient society in digitalized countries such as Norway we need to develop regulatory regimes that are stringent enough to be followed, but also flexible enough to adapt to the changing threat landscape. This rapid and continuous change of environment makes a rule-compliance regime alone, hopeless. Then again, a risk-based regime is too reliant on trust which makes it extremely vulnerable. Therefore, the rule-compliance regime provides an advantage as businesses are required to follow certain rules. As Hopkins (2011) pointes out:

> "… risk-management offers very little guidance to end point decision-makers; they need rules to guide their decisions. Accordingly, it is important, even within a risk management framework that risk-management be translated into rule compliance for end point decision-makers, where possible." (Hopkins, 2011, p. 110)

If societies shall be able to *prepare for, adapt to, withstand, and recover* from cyberterrorism we need to develop a dynamic, but stringent legal framework. This could for instance be based on the Norwegian NSA. Here, the rules should be generic, but also include clauses that allow for changes according to the threat landscape. Thus, as we already know what the threat is businesses and governments can focus on securing those digital vulnerabilities that can be exploited.

4. Conclusion

The complex nature of wicked problems such as terrorism makes it hard to develop effective countermeasures. As there is no right or wrong way in how to prevent terrorist attacks from happening, various actors tend to confront the phenomenon in different ways.

Regulation is one step towards the right direction. By establishing a regulatory foundation that governments and security agencies can work from it facilitates for the process of building resilient societies. Despite this, the risk-based regime should be combined with a rule-compliance regime when countering wicked problems such as cyberterrorism.

I believe the phenomenon is an emerging threat that governments, businesses, peoples, and individuals will have to deal with in the future. Regardless of future actors' motives and methods, a combination of two regimes may be the best way to build a resilient society as the advantages in one partly outweighs the challenges in the other.

Bibliography

Almklov, P. G., Antonsen, S., Størkersen, K. V., & Roe, E. (2018). Safer societies. *Safety Science*, *110*, 1–6. https://doi.org/10.1016/j.ssci.2018.03.018

CISA. (2016, February 25). *Cyber-Attack Against Ukrainian Critical Infrastructure | CISA*. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

Clarke, R. A., & Knake, R. K. (2014). *The Next Threat to National Security and What to Do About It*. 140.

Dalgaard-Nilsen, A. (2020). *Evaluering av politiets og PSTs håndtering av terrorhendelsen i Bærum 10. August 2019* (p. 262). https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/al-noor---terrorhandlingen/evaluering_terrorhendelsen_i_baerum_01072020_original_digital.pdf

Fischbacher-Smith, D. (2016). Framing the UK's counter-terrorism policy within the context of a wicked problem. *Public Money & Management*, *36*(6), 399–408. https://doi.org/10.1080/09540962.2016.1200801

Hopkins, A. (2011). Risk-management and rule-compliance: Decision-making in hazardous industries. *Safety Science*, *49*(2), 110–120. https://doi.org/10.1016/j.ssci.2010.07.014

Ivanova, K., & Sandler, T. (2007). *CBRN Attack Perpetrators: An Empirical Study*. 22. https://doi.org/10.1111/j.1743-8594.2007.00051.x

Jore, S. H. (2019a). Standardization of terrorism risk analysis: A means or an obstacle to achieving security? In *Standardization and Risk Governance: A Multi-Disciplinary Approach* (1st edition, pp. 150–165). Routledge. https://www.taylorfrancis.com/books/e/9780429290817/chapters/10.4324/9780429290817-12

Jore, S H. (2015). *Challengers of Building Societal Resilience through Organizational Security Risk Management*. 9.

Jore, S. H. (2019b). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174. https://doi.org/10.1007/s41125-017-0021-9

Jore, S. H. (2019c). Ontological and epistemological challenges of measuring the effectiveness of urban counterterrorism measures. *Security Journal*. https://doi.org/10.1057/s41284-019-00221-6

Jore, S. H. (2019d). The Multifaceted Aspect of Uncertainty – the Significance of Addressing Uncertainty in the Management of the Transboundary Wicked Problem of Terrorism. *Proceedings of the 29th European Safety and Reliability Conference (ESREL)*, 4044–4051. https://doi.org/10.3850/978-981-11-2724-3_0622-cd

Justis- og beredskapsdepartementet. (2019, January 1). *Lov om nasjonal sikkerhet (sikkerhetsloven)—Lovdata*. Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. *IEEE Security Privacy*, *9*(3), 49–51. https://doi.org/10.1109/MSP.2011.67

Lyse Konsern. (2020). *Beredskap for Lyse*. Lyse Konsern. https://www.lysekonsern.no/beredskap/

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

Nacos, B. L. (2019). *Terrorism and Counterterrorism: International student edition*. CRC Press.

NSM. (2020). *Risiko 2020* (Risiko). Nasjonal Sikkerhetsmyndighet.

Sassard, T. B., Sophie. (2016, July 15). A white truck, bodies fly, and a world of tears in Nice. *Reuters*. https://www.reuters.com/article/us-europe-attacks-nice-hospital-idUSKCN0ZV0G9

Theohary, C. A., & Rollins, J. W. (2015). Cyberwarfare and Cyberterrorism: In Brief. *Cyberwarfare and Cyberterrorism*, *7–5700*, 15.

Vilhelm, N. (2015, April 1). *Digital sårbarhet i kritisk infrastruktur.* Nasjonal Sikkerhetsmyndighet. https://esra.no/wp-content/uploads/2015/04/1-Vilhelm-Nasjonal-Sikkerhetsmyndighet.pdf

Weinberg, L., Pedahzur, A., & Hirsch-Hoefler, S. (2004). The Challenges of Conceptualizing Terrorism. *Terrorism and Political Violence*, *16*(4), 777–794. https://doi.org/10.1080/095465590899768

Zeller, M. (2011). Myth or reality—Does the Aurora vulnerability pose a risk to my generator? *2011 64th Annual Conference for Protective Relay Engineers*, 130–136. https://doi.org/10.1109/CPRE.2011.6035612

Zetter, K. (2016, March 3). Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *Wired*. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/