Contextual Cyber Securitisation

A Case Study of Russian Cyberattacks against Ukraine

Universiteit Leiden

INTERNATIONAL RELATIONS

MASTER THESIS

Louis Léonet

July 2019

Supervisor: Matthew Frear

Page intentionally left blank

Table of Contents

Introduction and purpose of this paper

Nowadays, cybersecurity – and all its related notions: cyber defence, cyberspace, cyber warfare, hacking, etc. – is a common term, appearing on a regular basis in traditional and modern media. The term originates from the Critical Infrastructure Working Group, a US inter-agency unit set up in 1995 and tasked with investigating threats to the connected assets of the country.[1] The turning point for the political interest in such matters can however be traced further back to 1984 and the adoption of the confidential directive NSDD-145 "National Policy on Telecommunications and Automated Information Systems Security" ordered by President Reagan, the first policy document of significance addressing the dangers of compromised computer networks.[2]

Since then, the scope and magnitude of information and communication technology (ICT) grew at an unfathomable speed, while shaping societies highly dependent on interconnected networks and affecting every sector of the global socio-economic landscape. As technological progress brought significant changes and improvements to our everyday lives, its threat and security dimension evolved at a matching, if not greater pace.

Cybersecurity is the generic concept covering all measures taken to combat threats looming in what we generically call "cyberspace" but that impact the material world and living people in a very tangible way. Identity thefts, data leaks, ransomwares,[3] malicious codes[4] of all natures that rely on Internet networks have been increasingly frequent and caused damage to millions, costing billions to companies and individuals across the world and became a hot topic of discussion in past few years, repetitively making the headlines.

We can re-use a 1991 definition by the US Computer Science and Telecommunications Board (CSTB), still valid today and that concisely encapsulates this broad concept. It defines security as:

> "[T]he protection against unwanted disclosure, modification, or destruction of data in a system and also [to] the safeguarding of systems themselves."[5]

The Copenhagen School, while widely recognised as a prominent approach to addressing security and its political effects, originally dismissed cybersecurity as a sector on its own,

[1] F. Kaplan, *Dark Territory: the Secret History of Cyber War*, Simon and Schuster Paperbacks (2016), p. 40-46

[2] *Ibid*, p. 1-2: we could go further back to the 1960's, at the initiation of ARPANET, the ancestor of today's Internet, developed by the American Advanced Research Projects Agency, triggering similar worries in a few minds: *see ibid.*, pp. 7 *et seq.*

[3] Definition: a ransomware is a subtype of malware that encrypts the data on a victim's computer, rendering it inaccessible, and demanding payment – often in the form of a cryptocurrency such as Bitcoins – in order to have it decrypted and accessible again. The most famous ransomwares were CryptoLocker (2014) and WannaCry (2017): *see* https://searchsecurity.techtarget.com/definition/ransomware

[4] Generally called *malware*: contraction for malicious software, it encompasses all programmes or files developed and/or used with the intent to cause harm, such as: stealing, encrypting or deleting data, altering or hijacking computers' essential functions, monitoring users' activity unbeknownst to them, etc. Most commonly known types of malware include viruses, worms, Trojan horses, spyware and ransomware: *see* https://searchsecurity.techtarget.com/definition/malware

[5] Computer Science and Telecommunications Board (CSBT), *Computers at Risk: Safe Computing in the Information Age*, report, Washington, DC: National Academy Press (1991), p. 2

subordinating it domains such as the military, the environment, the economy or even religion.[6]

This thesis aims at disproving this statement while addressing the shortcomings of the traditional approach to securitisation. For that purpose, this thesis is structured in two chapters. Chapter I addresses the theoretical framework for the securitisation theory and provides an altered framework compensating for said shortcomings. More specifically, it claims the need to move past the *speech act* philosophy as the central element of the theory and include more defining factors, in an attempt to provide a more broadly applicable framework, especially with regards to the cybersecurity sector and relying on contextual components.

In the second chapter, this reviewed securitisation theory is applied to a case study: the recent series of cyberattacks perpetrated by Russia against Ukraine. This practical case's purpose is to structure the development of framework for what we call *cyber securitisation.* Hence, theoretical claims and concrete example are intertwined in order to provide a concrete support to the abstract thinking while testing the claims made in this paper.

This thesis is not a technical piece; hence no specific knowledge is required. When technical elements are mentioned, a definition or a reference will be provided.

[6] L. Hansen & H. Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, International Studies Quarterly, vol. 53 (2009), p. 1156; B. Buzan, O. Wæver and J. de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers (1998), p. 25

I. Theoretical Framework: the Securitisation Theory

The first Chapter aims at identifying the key elements of the securitisation theory, its boundaries and prepare the groundwork for its application to the cyber domain. To that end, the Chapter will be divided in three sections: Section A identifies the roots of security studies within the realist tradition; Section B focuses on the securitisation theory, according to the Copenhagen School of thought and; Section C provides a critical analysis of the theory and highlights its shortcomings, structured around the axis that the speech act should not be the primary defining factor of security. It provides the groundwork for an alternate framework applicable to the cybersecurity sector.

A. Roots of Security Studies

There is a long-standing tradition of realist thinking in security studies, and most theoretical strands that derived from it brought new ideas for framing security in the social studies. Significant literature and research on the different declinations of realism occurred over the Cold War period and is thus influenced by the markers of the international political landscape of the time: bipolarity, nuclear deterrence, mutually assured destruction and state survival to name a few.[7] Since the end of the Cold War era, the realist landscape has been subject to tremors and new divergences emerged. Furthermore, the field suffers from the Western-centric nature in the security literature.[8]

Countless analyses and critiques were developed by outstanding scholars on the evolution of this field and how to apply the strands of realism – and other theoretical frameworks – to modern-day political developments. This thesis will not engage in such an endeavour, and the following paragraphs will simply help locating its focus, the theory of securitisation, itself a part of the sub-family of security studies, on the wide spectrum of international relations theories of realist descent.

Classical realists like Morgenthau argued that human behaviour, in all its imperfections, is at the core of power politics while international relations follow certain universal laws pertaining to human nature. [9] On the other hand, neo-realists offer a more systemic approach, considering that structures at national and international levels affect the actions taken in the global order and how they impact political currents.[10] The difference between the two thus lies in their perception of what the origin for the causes of international shifts and changes is.

[7] K. Krause, *Critical Theory and Security Studies: The Research Programme of Critical Security Studies,* Cooperation and Conflict, vol. 33(3) (1998), p. 301

[8] *See e.g.* N. Bubandt, *Vernacular Security,* Security Dialogue, vol. 36 (3) (2005); C. Wilkinson, *The Copenhagen School on Tour in Kyrgyzstan: Is Securitisation Theory Useable outside Europe?,* Security Dialogue, Vol. 38 (1) (2007)

[9] K. Jørgensen, *International Relations Theory: A New Introduction*, New York: Palgrave Macmillan (2010), p. 86, citing Morgenthau's *Politics among Nations* (1954)

[10] B. Buzan, *The Timeless Wisdom of Realism?, in* S. Smith, K. Booth & M. Zalewski, (eds.), *International Theory: Positivism and Beyond,* Cambridge University Press (1996), p. 51; J. Sterling-Folker, *Realism and the Constructivist Challenge: Rejecting, Reconstructing, or Rereading,* International Studies Review, vol. 4(1) (2002), p. 77; Jørgensen, *International Relations Theory* (2010), p. 84

The common ground for all realist theories is the acceptance that structures exist outside of the scope of influence of human action, and that the central actor in international relations is the State, pursuing the maximisation of its relative power to guarantee its own interests in order to survive.[11] This is the basis for the realist reasoning that states are rational actors, which permits an objective analysis of international relations.

Realism, regardless of its declination, has dominated international relations studies for decades and security studies is no exception. With States at the centre of international politics, a system inherently anarchic that is regulated by forces they produce, assessing the threats posed by others, in an effort of self-preservation.[12] Two essential theories emerged from this chaotic framework and still act as pillar of modern security theories: *the security dilemma* and the *balance of power.*

The security dilemma amounts to the idea that by pursuing security for itself, the actions it takes will generate insecurity for other, competing actors (*i.e.* States).[13] The notion of balance of power refers to the attempt of States to attain a certain level of order in the anarchic landscape of international relations, by either acting *externally* and having weaker States to coalesce[14] (for instance forming an alliance or regional organisation), or *internally* via political, military or economic policies to match other actors.[15] These elements translated into theoretical frameworks with an underlying tone of conflict and competition between States, a central aspect of security studies development throughout the Cold War, as it "emphasize[s] the competitive and conflictual side of international relations".[16] This supports the claim that security studies are derivative from the realist approach.

In the context of this thesis, we lean towards the neo-realist approach as it applies well to the thematic of cybersecurity and cybersecurity, given the relevance of a systemic-level analysis while discarding human behaviour as an influential factor.[17] This may appear counter-intuitive, as one might argue that humans are key elements in the cyberattack and cyber response exchange: a single hacker can cause tremendous amounts of damage and people are often referred to as the "weak link" of an organisation security system.[18]

Nonetheless, the idea that the State is the main and rational actor in an international, conflict-driven landscape, where agents struggle for security by implementing policies in response to perceived threats and other powers' capabilities[19] is very fitting to the interconnected and

[11] M. Mastanduno, *Preserving the Unipolar Moment: Realist Theories and U.S. Grand Strategy after the Cold War*, International Security, vol. 21(4) (1997), p. 52

[12] Buzan, *Timeless Wisdom of Realism?* (1996), pp. 50-51

[13] K. Fierke, *Critical Approaches to International Security*, Cambridge Polity Press (2007), p. 18

[14] Fierke, *Critical Approaches* (2007), p. 18

[15] Y. Wang, *China's Response to the Unipolar World: The Strategic Logic of Peaceful Development*, Journal of Asian and African Studies, vol. 45(5) (2010), p. 556

[16] Buzan, *Timeless Wisdom of Realism?* (1996), pp. 50-51

[17] *Ibid.*, p. 51; Sterling-Folker, *Realism and the Constructivist Challenge* (2002), p.77

[18] *See e.g.:* Kaspersky, "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within", available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/

[19] *See* Walt's *balance of threat* theory which accounts not only to States' capabilities but also *intentions*: S. Walt, *Alliance formation and the balance of world power*, International Security, vol. 9(4) (1985), pp. 9-10

chaotic place that is cyberspace. The ideas of balance, threats and central authority greatly align with the complex relations between a multitude of actors and their pursuit for security against a vast, often blurred constellation of adversaries.

B. Securitisation and the Copenhagen School

Amidst the above-described approaches and schools of thought, stemming from neo-realist security studies as well as constructivist constructs, emerged a theory dedicated to the understanding of security events: the *securitisation theory*. Considered the most prominent approach to security, this theory is the conceptual pillar of what is called the *Copenhagen School* of thought,[20] which gained its name from its originators: Ole Wæver, Barry Buzan and Jaap de Wilde who worked at the Copenhagen Peace Research Institute at the time.[21] They define securitisation as a:

> "[D]iscursive process through which an intersubjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat."[22]

In other words, "saying security"[23] is a *process* where an authority identifies a situation and characterises it as threat. The essence of security therefore resides with the discourse surrounding the constitutive elements of securitisation. From the above-mentioned definition, we extract four elements on which this process rests: (1) an existential threat over (2) a referent object, brought to existence via (3) a discursive process – *speech act* – and requiring (4) urgent and exceptional measures.

The speech act is the defining characteristic of the Copenhagen School's securitisation theory. Wæver argued that security itself is to be regarded as a speech act, and "the utterance itself is the act".24 The notion is well described by Judith Butler who argued that the speech act holds productive power, meaning that it can create its own meaning and affect social and societal relations. The concept, called performativity, thus confers the speech act the power to create

[20] The securitisation theory developed into two main strands: the Copenhagen School, our focus, and the *Aberystwyth School*, led by scholars like K. Booth and R. Jones. It has roots in Marxism and neo Gramscian critical theory, opposing the state-centric approach and putting human emancipation at its centre: *see* K. Booth, *Security and Emancipation*, Review of International Relations, vol.17 (1991); R. W. Wyn, *"Message in a Bottle"? Theory and Practice in Critical Security Studies*, Contemporary Security Policy, vol. 16 (1995).

[21] B. McSweeney, *Identity and Security: Buzan and the Copenhagen School*, Review of International Studies, vol. 22 (1996), p. 81

[22] B. Buzan & O. Wæver , *Regions and Powers: The Structure of International Security*, Cambridge University Press (2003), p. 491

[23] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1158

[24] O. Wæver , *Securitisation and Desecuritisation, in* R. Lipschutz (ed.) *On Security*, Columbia University Press (1995), pp. 54-55

authority and change internally, notwithstanding external elements,25 and joins the approach taken by Wæver.26

The two other components involved in the discursive act are the securitising actor and the audience. As evoked already, security according to the Copenhagen School is an intersubjective process in which an actor performs a securitising move by uttering a speech aimed at a target audience that must accept it as such. 27 Traditionally, the actor is the State in its governing function while the audience can amount to the population, with an intrinsic approval power.

As the threat element is construed via this act of discussion, the threat does not need to be objectively real or possible; all that is required is that it is perceived as existing from the securitising actor's perspective. In other words, "a threat is no longer simply assessed but its interpretation and representation is 'negotiated' between an actor and the relevant audience."[28] The referent object of the threat is often the State itself but this time in a broader, societal sense, amounting to a structure and a population within it.[29]

If the target audience accepts the message, recourse to emergency measures that fall outside normal political practice are justified.[30] In a way, securitising an event helps identifying the actor with such power, the level of authority it holds towards a particular audience as well as the requirements for an alleged event to be considered a security issue or threat in political discourse.[31] Wæver encapsulates the conclusive aspect of securitisation in one sentence:

> "By uttering 'security', a state-representative moves a particular development into a specific area, and thereby claims a special right to use whatever means are necessary to block it."[32]

Two takeaways from this initial description of the securitising process will serve as conclusive statements.

First, the idea of elevating an issue above normal politics once it has been labelled a 'security event' comforts the realist claim that security is a distinct field in political practice, granting such issues an exceptional status among policy concerns.[33]

[25] J. Butler, *Performativity's Social Magic*, *in* T. Schatzki & W. Natter (eds.) *The Social and Political Body,* New York: Guilford Press (1996), pp. 30-31

[26] *See* Wæver , *Securitisation and Desecuritisation* (1995) but also; O. Wæver , *The EU as a Security Actor: Reflections from a Pessimistic Constructivist on Post Sovereign Security Orders*, *in* M. Kelstrup & M. Williams (eds.) *International Relations Theory and the Politics of European Integration,* London: Routledge (2000)

[27] Buzan, Wæver and de Wilde, *New Framework for Analysis* (1998), p. 24

[28] H. Stritzel, *Towards a Theory of Securitisation: Copenhagen and Beyond*, European Journal of International Relations vol. 13(3) (2007), p. 363

[29] Fierke, *Critical Approaches* (2007) pp. 104-105; Buzan, Wæver & De Wilde, *New Framework for Analysis* (1998), p. 24

[30] Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), p. 24

[31] *Ibid.*, pp. 25-30

[32] Wæver , *Securitisation and Desecuritisation* (1995), p. 55

[33] *Ibid.*, pp. 51-52; Stritzel, *Copenhagen and Beyond* (2007), pp. 360-361

Second, it must be borne in mind that securitisation is a negative process, as one must avoid as much as possible to bring an event in the realm of security, removing it from the normal course of politics. Wæver developed a counter-mechanism for what he named *de-securitisation*, which is aimed at resolving an issue potentially *securitis-able* without resorting to emergency measures.[34]

There is much debate surrounding the securitisation theory and a lot can be argued about whether it is primarily rooted in the neo-realist or the constructivist tradition, how the various theoretical concepts developed in the contested field of security studies[35] have impacted (or not) the Copenhagen School of thought. Nonetheless, the above description should set a sufficient, broadly acceptable theoretical framework for the purpose of this thesis. The two following sections provide a critical assessment of certain components of securitisation and analyse how to apply it to the field of cybersecurity.

C. Limitations of the Copenhagen School: Beyond the Speech Act

The Copenhagen School and the securitisation theory are subject to multiple critiques that merit debating, but this thesis shall focus on the central pillar supporting its framework: the speech act. It aims to prove how it can restrict – and even distort – the conduct of an analysis by preventing the establishment of coherent, systematic framework.

It is important at this point to remember that there is no single theory that could explain the 'everything' of a subject, and securitisation cannot pretend to be an exception in the field of security studies, as it has been subject to criticism for attempting a "shorthand for the construction of security."[36]

It is the opinion assumed by this thesis that attributing such a defining – or *performative* – power to speech alone eludes the impact of many other significant factors. Also, the idea that a single actor, usually a state agent (*i.e.*: the government), can propel an event into a particular realm and categorise it as a threat poses risks depending on the nature and agenda of the securitising agent.[37]

Stritzel decorticates the approach as described above and opposes its model, which he qualifies as *internalist* – that is following the speech act model and theory of performative utterances – to an *externalist* understanding.[38]According to the first model, the securitising agent has a dual hat: on the one hand, it is performing a securitising move which amounts to

[34] *Ibid.*, pp. 56-57; Buzan, Wæver & De Wilde, *New Framework for Analysis* (1998), p. 35.

[35] For more on this issue, *see* S. Smith, *The Contested Concept of Security*, *in* K. Booth (ed.), *Critical Security Studies and World Politics*, Lynne Rienner Publishers (2005), pp. 27 *et seq.*

[36] M. McDonald, *Securitisation and the Construction of Security*, European Journal of International Relations, vol. 14(4) (2008), pp. 580-581.

[37] In the cybersecurity theme, one might first think of authoritative regimes such as China: *see* Y. Yuang, "The Great Firewall of China: Web of Control", Financial Times (12 March 2019), available at: https://www.ft.com/content/e19b3022-40eb-11e9-9bee-efab61506f44, but democracies also exercise excessive powers, like the US: "Privacy and Surveillance Post-9/11", American Bar Association (30 June 2017), available at: https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11/

[38] Stritzel, *Copenhagen and Beyond* (2007), pp. 360-361.

an interpretation of an event, while it negotiates its threatening nature with a target audience or representation and, if said audience accepts it, the *trilogue* is complete, legitimising the use of emergency measures by the actor.[39]

Stritzel rightfully points the evasiveness of this relation, following this limited interpretation-negotiation-acceptance (or rejection) sequence. However, although his suggestion to develop a more dynamic intersubjectivity between these elements is relevant, it occults a more significant dimension of the problem by still maintaining the speech act philosophy at the centre of the process.[40]

This is where the externalist approach is relevant. It is essential to keep in mind that this analysis does not seek to eliminate the speech act or reduce it to a marginal component of the securitisation process. The goal is to bring forward other elements to articulate alongside the speech act and reshape the theory by adding a new dimension – or *plane* – to it.[41]

The first element to address is the facilitating conditions, a notion that encompasses three items: (1) the security dimension of the speech, (2) the authority relation between the securitising actor and the target audience and (3) the nature and characteristic of the perceived threat. The notion of facilitating conditions exists in the Copenhagen literature[42] but is mostly marginal, even contradictory with the discursive approach.[43] By following the conceptual line of each of them, we observe a direct relation with each of the traditional elements of the securitisation process. From these relations, we will address the shortcomings of the Copenhagen School approach.

Starting with the speech act philosophy, the supporting pillar of the theory and main object of this thesis' theoretical critique, I argue that the ability to generate meaning essentially based on a discursive act is dismissive of too many highly influential elements. While the speech act plays a key role in the formation of policy and is one factor helping determine the threatening nature of an event.

On the other hand, as the speech act is framed by an actor attempting securitisation of what it interprets as a threat, the *grammar* surrounding the issue – or, more broadly, its sector – and the semantics employed by the securitising agent and other facilitating actors (*see below*) will either increase or hinder the chances of acceptance from the targeted audience.

Secondly, with regards to the role of the audience, as it is described in the main writings on securitisation, is exaggerated. The securitising actor, by its inherent authority and attributions,[44] will more often than not have pre-determined whether an event is to be considered a threat, and thus dealt with it in the realm above politics. In other words, there

[39] *Ibid.*, p. 363; Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), p. 25

[40] *Ibid.*, pp. 362-363; *see also*: Wæver , *Securitisation and Desecuritisation* (1995), pp. 44 *et seq.*; Fierke, *Critical Approaches* (2007), pp. 104-105.

[41] Stritzel, *Copenhagen and Beyond* (2007), p. 363.

[42] Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), pp. 31-33

[43] *See* Stritzel, *Copenhagen and Beyond* (2007), pp. 365-367

[44] Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), p. 31-32: on actors in "positions of power […] by having the power to define security."

exists no real negotiation between a State-level actor and the general population as an actor to be convinced in order to become legitimate.[45]

That does not amount to say that civil society and the population play no role in defining security. Simply, we should stop considering the components as static and segregated and rather view them as dynamic, with a potential to play multiple roles in the process. Actors, which include securitising agents, the audience and the recipient object, overlap and share or exchange places.[46] They belong to a broader framework that puts agents and structures in relation within which the object of security can be discussed.[47] Hay describes this relation as follows:

> "Agents are situated within a structured context which presents an uneven distribution of opportunities and constraints to them. Actors influence the development of that context over time through the consequences of their actions. Yet, at any given time, the ability of actors to realise their intentions is set by the context itself."[48]

This idea implies a stronger reliance on social interactions and leads to the third and last component: the characteristics of the alleged threat itself. The externalist approach insists on the idea of facilitating factors that affect the securitisation process concurrently with the intersubjective speech act. In other words, *context* can also create meaning. Context can be understood as the conditions outside the control of the actors, such as the political landscape, the economic situation or the climatic changes. It can also include the nature of the relations between the actors, especially the State authority and its citizens.

By superposing the previous propositions, we can establish a skeleton for what Stritzel defines as an *embedded* model of security. Securitising actors, their discourse and their relations are embedded in "broader social and linguistic structures" where meaning and power can be created relatively to the object, sector or general context.[49] This approach relies on a more structural basis, which goes counter to Wæver's original framework,[50] although, he also hinted towards the potential of a more embedded securitisation.[51]

The externalist, embedded version of the theory provides a much more flexible and generally applicable framework that permits a shift of power relative to the context of social relations and objective changes in the political environment. Articulating security becomes more fluid and counter-discourses may exist which is beneficial when the consequence of a successful securitisation is to take exceptional/emergency measures.[52]

[45] *Ibid.*, p. 41: on the audience amounting to "those the securitising act attempts to convince".

[46] Stritzel, *Copenhagen and Beyond* (2007), pp. 366-367.

[47] *Ibid., see also:* McSweeney, *Buzan and the Copenhagen School*, (1996)

[48] C. Hay, *Political Analysis: A Critical Introduction,* New York: Palgrave (2002), pp. 116-117

[49] Stritzel, *Copenhagen and Beyond* (2007), pp. 367-368.

[50] Wæver, *The EU as a Security Actor* (2000), p. 252

[51] O. Wæver, *Identity, Communities and Foreign Policy, in* L. Hansen and O. Wæver (eds.), *European Integration and National Identity,* London: Routledge (2001) p. 29

[52] *Ibid.*,

In addition to this reviewed framework, we wish to highlight two key evolutions from the original Copenhagen School prescriptions: one is the slight distancing from the traditional State-centric nature of security, which allows for the inclusion of new actors that can compete with the State as holders of power and authority. While modest, this is a progress upon which we can build a more comprehensive framework:

> "Security is an area of competing actors, but it is a biased one in which the state is still generally privileged as the actor historically endowed with security tasks and most adequately structured for this purpose."[53]

The second concerns the broadening of the range of issues that can be securitised, beyond traditional defence and military topics, to include terrorism, immigration or the environment to name a few.[54] These *sectors* – military, political, environmental, societal economic and religious being the main ones – can be defined as:

> "[L]enses or discourses rather than objectively existing phenomena and they are defined by particular constitutions of referent objects and types of threats as well as by specific forms of 'grammar' of securitisation".[55]

Wæver originally opposed this idea, arguing that:

> "Widening along the *referent object* axis - that is, saying that 'security is not only military defense of the state, it is also x and y and z' - has the unfortunate effect of expanding the security realm endlessly, until it encompasses the whole social and political agenda."[56]

However, he also suggested alternatives to expand the framework by inclusion beyond the military threats, as long as certain features would remain: urgency, State power and authority to employ exceptional measures, and a (perceived) threat disturbing the normal conduct of politics.

This brings us to the last theoretical component of the first chapter: securitising cyberspace.

[53] Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), pp. 36-37

[54] McDonald, *Securitisation and the Construction Of Security* (2008), p. 567

[55] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1157, referring to Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), p. 27

[56] Wæver , *Securitisation and Desecuritisation* (1995), p. 38

II. Case Study: Russian cyber operations against Ukraine

While in the formative years of the securitisation theory, cybersecurity constituted a failed attempt at securitisation,[57] it is today unanimously recognised as *the* security issue in perpetual expansion. Rachel Yould claimed already fifteen years ago that "IT may be the common underlying factor upon which all security sectors are destined to converge."[58] She could hardly have been more accurate: it is difficult today to think of a single domain of human activity that is not reliant – often heavily – on ICT structures.

The question here is not to question the security nature of cybersecurity or its stance among the principle sectors: it is evident today that it holds a singular position as it affects all the above-mentioned sectors, in particular the military, the economy, the societal and the political sectors. Nonetheless, blurred exist lines between security issues threatening the State and its population and fraudulent, criminal activities falling below such threshold of "existential threat". While some acts in cyberspace may appear trivial, like conducting spear phishing campaigns and stealing passwords, they can be an initial step for large-scale disruptive, even destructive hacks with systemic consequences for governing powers and the global economy.

The purpose of this second chapter is to directly test the securitisation approach developed in the first chapter to a specific, real-life scenario in the cybersecurity domain, highlighting the relevance of a more systematic, external approach to defining security events with a cyber-dimension.

It is structured as follows: Section A explains why the topic of Russian cyberattacks against Ukraine was selected for this study; Section B provides a general background of both the geopolitical context of the Ukrainian conflict as well as the timeline for the cyber operations relevant to our analysis, focusing on three key instance; Section C develops a new framework for the securitisation of the cyber sector based on the case at hand.

This last section successively reviews the uniqueness of the cyber sector, the relations of securitising actors and referents, and then concludes on the notion of contextual securitisation.

A. The rationale behind the choice of topic

Firstly, the armed conflict involving Russia and composed of all the elements of modern day warfare – involving non-state armed groups, invasion tactics, election meddling and economic pressure, all of which gathers the political, military and economic factors that characterise a situation as a *bona fide* modern armed conflict between States. Furthermore, the international community, in the form of international organisations like the European Union and NATO but also foreign powers like the US, is firmly involved in the whole issue.

[57] Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), p. 25

[58] R. Yould, *Beyond the American Fortress: Understanding Homeland Security in the Information Age, in* R. Latham (ed.), *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security,* New York: The New Press (2003), p. 78

These elements permit to grant an undeniable security status to the overall context as well as align with the Copenhagen School's general traits: having States and multinational organisations as centres of power – or *authority* – while maintaining a classic Western-centred perspective with Russia as the hostile actor of the story.[59]

While these factors can be discussed as they restrict the broader applicability of the Copenhagen School's theory – should be addressed if one attempts to transform it into a more systematic framework of analysis – for the sake of our argument, which is to demonstrate the need to go beyond the speech act as the core component of the securitisation process with regards to cybersecurity as a field on its own, giving in to those limitations will permit to challenge my hypothesis against a topic where other variables are not creating superfluous *noise* or generating unwanted contradictions.

The recent attacks on the Ukrainian infrastructure provide an ideal testing scenario to that end, allowing to focus on a particular type of cyber operation with easy-to-grasp consequences in the material world, preventing unnecessary widening of the scope to other cases (*i.e.*, data theft, industrial espionage, etc.) while being composed of multiple occurrences allowing for comparison and identification of patterns.

B. Factual background

Geopolitical background of the conflict

In January and February 2014, the Euromaidan protests in response to the rejection of the Ukraine-EU Association Agreement by President Yanukovych take place.

On March 16th 2014, Crimea is annexed by Russia via an unrecognised referendum, following the occupation by pro-Russian combatants dubbed "little green men". The next month, hostilities begin in Eastern Ukraine with significant casualties and on June 17th, the MH17 flight is downed over Ukraine, while its investigation brought damning evidence against Russia and the separatists, the international reaction was underwhelming.

In September 2014, then February 2015, ceasefire agreements are concluded in Minsk, with barely any effect on the conflict. Afterwards, pro-Western figures take over the majority of the political landscape in Ukraine.[60]

In April 2016, NATO deploys forces to Eastern Europe - Estonia, Latvia, Lithuania, and Poland – in a deterring move towards Russia, also aiming at reassuring European allies, especially Baltic States. In September 2017, US Tank brigades were stationed in Poland to bolster the Alliance's presence.[61]

[59] Securitisation, and security studies in general, provide a Western-centric status to security (originally developed during the Cold War): *see* Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1158,

[60] K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCDCOE (2015), p. 10

[61] Global Conflict Tracker, Council on Foreign Relations, available at: https://www.cfr.org/interactive/global-conflict-tracker/conflict/conflict-ukraine

The conflict dragged on over the past years and became one of several background geopolitical situations that draw less attention as time goes by, overshadowed by new international events and crises; the election of Donald Trump and its ensuing diplomatic ventures, the return of nuclear fears with North Korea and Iran, the rise of international terrorism and downfall of ISIS, as well as challenges directly affecting Europeans, such as Brexit or the rise of populist forces.

Last April, Volodymyr Zelensky was elected as the new president of Ukraine, in what some see as a protest vote against Porochenko, elected in 2014 after the removal of Yanukovych in the midst of Euromaidan. However, this barely registered as a major event despite occurring in a still ongoing conflict at the EU's doorstep.[62]

Amidst these events with very tangible effects, including people losing their lives, an historic moment occurred in the dark – *literally*.

Cyberattacks against Ukraine: three milestones

BlackEnergy3 / KillDisk: the first power-grid killer

On 23 December 2015, the Prykarpattyaoblenergo control centre which distributes power across the Ivano-Frankivsk region, in Western Ukraine, saw its industrial systems taken over by an external actor and forcibly shut down, alongside two other centres. This caused over 230, 000 citizens to lose light and heat in a brisk winter, and became the first ever registered hack to disable a power grid.[63] And while power was restored in a matter of hours, it took months to fully restore the control centres to their initial operational levels.[64]

The tool employed by the hackers are known as *BlackEnergy*, a snooping programme that infiltrated the Ukrainian energy companies' networks via the use of spear phishing campaigns – sending fake e-mails to employees with clickable content, downloading the programme on their machines if clicked – then propagating its data-wiping companion, *KillDisk*.[65]

Crash Override: stealthier, potentially deadlier

A year later, hackers this time targeted an electric transmission station in Kiev, causing a blackout affecting a fifth of the capital's power capacity, for roughly an hour. While this does not seem alarming, the evidence suggests that this could have been a test-run for what could be "the most evolved specimen of grid-sabotaging malware ever observed."[66] The security analysts investigating the hack indicated that this malware, firstly dubbed *Industroyer* and

[62] "Ukraine election: Comedian Zelensky wins presidency by landslide", BBC (22 April 2019), available at: https://www.bbc.com/news/world-europe-48007487

[63] K. Zetter, "Inside the cunning, unprecedented hack of Ukraine's power grid", WIRED (03 March 2016), available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

[64] *Id.*

[65] K. Wilhoit, "KillDisk and BlackEnergy Are Not Just Energy Sector Threats", TrendLabs Security Intelligence Blog (16 February 2016), available at http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats

[66] A. Greenberg, "'Crash Override': the malware that took down a power grid", WIRED (12 June 2017), available at: https://www.wired.com/story/crash-override-malware/

now better known as *Crash Override*, was specifically designed for physical system disruption.[67] There has been only one known antecedent case: *Stuxnet*, the US-Israel code deployed within Iran's Natanz nuclear facility and destroying enrichment centrifuges in 2009.[68]

The truly fearful development is that Crash Override can conduct automated attacks, while the BlackEnergy/KillDisk duo required manual execution from another terminal. This brings significant threat to power grids in Europe, the Middle East and the US.[69]

NotPetya: a global hit

Finally, in June 2017, the most devastating and widespread cyberattack in history took place, inscribing the name *NotPetya* in digital history. It started on the servers of a small Ukrainian software firm, Linkos Group. One of Linkos' contracts related to an accounting piece of software – M.E.Doc – which is used virtually by everyone in the country. Through the programme updates, hackers installed backdoor access on thousands of servers with M.E.Doc installed, in Ukraine and across the world.

Then, on June 27th, companies around the world saw their computer paralysed or shut down. Hours after it first surfaced in Ukraine, it spread across the world in what "was simply the fastest-propagating piece of malware we've ever seen."[70] Hospitals, factories, multinational companies, and transport and construction firms: all sectors were affected and even Russia's oil industry suffered from a boomerang effect. The resulting damage was over 10 billion USD, making it the costliest cyberattack ever, outclassing the infamous *WannaCry* ransomware unleashed a month before which was evaluated to have cost between 4 and 8 billion USD.

In short, NotPetya results from vulnerability in Windows operating systems dubbed *EternalBlue*. The name refers both to the vulnerability as well as the exploit allegedly weaponised by the NSA and part of the large scale leak perpetrated by the *Shadow Brokers*.[71] It allows hackers to remotely activate their code on an unpatched computer, which is already how WannaCry was spread. It was re-used in the NotPetya scenario in combination with an older programme called *Mimikatz* which basically allows extracting passwords once a machine is infiltrated. It could even access connected computers, which allowed the NotPetya

[67] A. Cherepanov & R. Lipovsky, "Industroyer: Biggest threat to industrial control systems since Stuxnet", Welivesecurity (12 June 2017), available at: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/; R. Lee, "CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids", Dragos, available at: https://dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/

[68] WIRED, "Crash Override"; *see* R. Langner., *To Kill a Centrifuge*, Report, The Langner Group (November 2013), available at: https://www.langner.com/to-kill-a-centrifuge/

[69] R. Lipovsky, "Seven years after Stuxnet: Industrial systems security once again in the spotlight", Welivesecurity (16 June 2017), available at: https://www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/

[70] Craig Williams, director of outreach at Cisco's Talos division, to WIRED: A. Greenberg, "The untold story of NotPetya, the most devastating cyberattack in history", WIRED (22 August 2018), available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[71] L. Hay Newma, "The leaked NSA tool that hacked the world", WIRED (07 March 2018), available at: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/

virus to move from one computer to another, even if the EternalBlue vulnerability had been patched.[72]

NotPetya takes its name after *Petya*, a ransomware that broke out in March 2016. While being very similar, NotPetya has significant differences: it spreads by itself while Petya required a user to (unknowingly) activate it; it encrypts much more components but most of all; it is *not* a ransomware. It asks the user to transfer Bitcoins in order to receive a decryption key but only provides a random number, while in fact having already destroyed the data beyond recovery, making it the most destructive and aggressive malware.[73]

Contrarily to the first two instances, NotPetya was not specifically targeting a power-grid or critical infrastructure nor was it focused on Ukrainian assets. However, the bleed effect, scope and extent of the damage it caused – including to banks, health services, and other vital services – and the fact it originated in Ukraine make it relevant to our study. Furthermore, researchers linked the NotPetya outbreak to BlackEnergy3 and Crash Override in the methods employed, tracing it to the same group: Sandworm, also known as Voodoo Bear or Telebots, strongly believed to be linked to Russian military services, with a special interest in targeting power grids.[74]

These three instances of cyberattacks with wide-ranging consequences occurred in the midst of cyber warfare campaigns that started roughly at the same time as the Ukrainian conflict, at an intensity rarely seen elsewhere. As Kenneth Geers, senior fellow at the Atlantic Council and NATO Cyber Defence advisor says: "Ukraine is a live-fire space."[75] Indeed, Russia has engaged in the most absolute display of hybrid warfare, on the battlefield of the Donbas and inside Ukraine's networks, perpetrating DDoS attacks,[76] sensitive data theft, disinformation / misinformation campaigns but also relying on data feed to support revolutionary troops by communicating enemy positions or disrupting the Ukrainian army's communications.[77] Such activities persist to this day.

[72] WIRED, "The untold story of NotPetya"

[73] J. Fruhlinger, "Petya ransomware and NotPetya malware: What you need to know now", CSO Online (17 October 2017), available at: https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

[74] J. Hultquist, "Sandworm Team and the Ukrainian Power Authority Attacks", FireEye (07 January 2016), available at: https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html; A. Greenberg, "Your guide to Russia's infrastructure hacking teams", WIRED (12 July 2017), available at: https://www.wired.com/story/russian-hacking-teams-infrastructure/

[75] L. Cerulus, "How Ukraine became a test bed for cyberweaponry", Politico (14 February 2019), available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/?fbclid=IwAR2YvS7Cq6zrcObPELejDyWBsJtF3MAXxy3PzgwI0ZcbDW9SGkEtC5vZyas

[76] A Distributed Denial of Service attack overloads a system with basic requests, paralysing it: https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack

[77] *See* K. Geers (ed.), *Cyber War in Perspective* (2015), p. 11.

C. Developing a dedicated framework for cyber-securitisation

The unique nature of the cybersecurity sector

The grammar[78] of the cybersecurity sector, that follows the externalist – embedded approach developed in Chapter I, must be established upon *pillars* that will act as the basis for a framework dedicated to the cybersecurity sector. The following subsection analyses three concepts extracted from securitisation literature: everyday security practice, the borderless nature of cyberspace and hypersecuritisation.

It must be pointed out that 'grammar' does not equal 'semantics', but rather that the lens we apply to this sector has generated a vernacular that connotes danger, urgency or hostility: cybersecurity, data *protection*, *critical* infrastructure, system *penetration*, *spear* phishing, virus, and worm, etc. One can immediately relate the impact of the sector's semantics to the notion of speech act.

Everyday security practice or the constant insecurity

Securitising cyber activities is different than securitising an issue like the nuclear Holocaust during the Cold War: while the latter evokes the extermination of the human race in a matter of moments, there is rather a sense of constant insecurity that is inherent to cyberspace and that can be grasped by the everyday person, from warnings against credit card fraud, privacy intrusions, data theft, etc.[79] It does not suffice to generate the interpretation of an existential threat to a referent, be it the State, the population / society or the private sector and its economic stability, but is enough to instil a fleeting sense of danger.

In the Ukrainian context, we bring this notion to an extreme degree: as described in the factual background, Russia conducts extensive, constant cyber operations. Hence, the population and government authorities perceive this insecurity to a higher degree, which could arguably suffice to be securitised and justify emergency measures.

In other contexts, we have witnessed the increase in threats to cybersecurity, alongside stronger and firmer responses in the political landscape in response to an anticipated growth in hostile actors' capabilities and numbers. For example, the US back in 2002 published its second CSBT report, warning that cyberattacks in the future would "compromise systems and networks in ways that could render communications and electric power distribution difficult or impossible, disrupt transportation and shipping, disable financial transactions, and result in the theft of large amounts of money."[80] It shows how discourse still plays a central role, yet insufficient by itself, in securitising an issue.

[78] Buzan, Wæver & de Wilde, *New Framework for Analysis* (1998), p. 27

[79] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1165

[80] CSBT, *Today and Tomorrow: Pay Now or Pay Later*, report, Washington, DC: National Academy Press (2002), p. 6; over the past decades, most States have repeatedly published similar documents with an ever more warning tone, with limited results.

This meets this thesis' approach that external factors and context play a significant role in 'successfully' securitising a cyber-related event.[81] Subsequently, this continuous idea of navigating in an inherently unsafe environment brings the individual closer to the issue, activating its ability to perceive a potential threat and seeing themselves as recipient to this threat. At this level however, the individual, even collectively should not be expected to carry a securitisation power but certainly creates a new dynamic in the relation it holds with another securitising authority over such issue. This will be further developed below in the subsection "Actors vs. referent objects."

Fluidity and cross-sector nature

We already mentioned how cybersecurity is global, cross-sector notion that impacts every aspect of modern life. In addition, parallels were made and shared features identified with most other security sectors: finance (technicality and relevance of private sector); the environment (planet-wide effect and irreversible nature); pandemics and epidemics (instantaneity but more containable); etc.[82]

With regards to the traditionally prime field of the Copenhagen School, the security / defence sector, it appears evident that superposing the features of everyday security practices and hypersecuritisation, which can trigger dramatic cascading effects across several sectors, "move[s] cybersecurity out of the realm of 'corporate security' or 'consumer trust' and into the modality of 'proper' national/societal security."[83] Furthermore, the transnational nature of networks pushes it higher as it can no longer be solely seen as a national security matter but as an issue that requires international cooperation.

We have seen the joint efforts of European Union Member States and NATO members following the devastating WannaCry and NotPetya, in order to design more efficient countermeasures against future outbreaks.[84] Unfortunately, as much as cooperation is needed in a borderless domain, States maintain a stance favouring their own interest – in a very traditional realist way.

Hypersecuritisation

This is a concept consisting in augmenting the intensity of the securitisation process by going beyond normal threat levels. Buzan describes it as a "tendency both to exaggerate threats and to resort to excessive countermeasures."[85] More a question of "degree" than of successful securitisation, this approach is complex to apply to real-life scenarios, even if we were to consider the scope of a large-scale cyberattack with irreversible damage in several sectors.[86]

[81] As a reminder, securitisation is not a positive process and one should aim at minimising the impact of an event, in a de-securitising effort.

[82] Hansen & Nissenbaum, *Digital Disaster* (2009), pp. 1164-1165.

[83] *Ibid.*, p. 1166

[84] *See* P. Pawlak, *Protecting and Defending Europe's Cyberspace, in* N. Popescu & S. Secrieru (eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies,* EUISS Chaillot Papers n° 148 (October 2018), pp. 110 *et seq.*

[85] B. Buzan, *The United States and the Great Powers: World Politics in the Twenty-First Century,* Cambridge: Polity (2004), p.172.

[86] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1164.

If we take the example of NotPetya which definitely fits this description, while there were warnings about the impending risk of a large-scale cyberattack[87] – notably one that would target critical infrastructures – what dismisses the practical application of hypersecuritisation is the impractical idea of "excessive countermeasures". Despite having seen (and anticipating) a multi-billion worth of damage from a single event, no countermeasure undertaken by public authorities could qualify as "excessive". In fact, barely any action was taken.[88] There are simply too many unknowns, starting from a non-irrefutable proof that Russia perpetrated it.[89]

However, by extracting the ideas of "instantaneity" posed by Denning[90] as well as from the cross-sector nature of cybersecurity threats,[91] we can apply the idea of hypersecuritisation to cyberspace as a pillar of its nature in that it can instantly create immense and irreversible damage. Indeed, as mentioned previously, the NotPetya malware was the fastest spreading worm ever recorded. To give an idea of its devastating speed, reports told that "it took 45 seconds to bring down the network of a large Ukrainian bank" while "a portion of one major Ukrainian transit hub […] was fully infected in 16 seconds."[92] In a few hours, it had gone global, affecting entities such as the Ukrainian government, French group Saint-Gobain, Danish shipping giant Maersk, FedEx, pharmaceutical company Merck or the British WPP advertising group, to name a few.[93]

Timely response, even in less extreme cases, still is an empty wish. If we consider the 2015 hack, the first of its kind, operators at the infected power station directly witnessed the unfolding of events on their screens, with no ability to act as the hackers had taken over and blocked every possible control, even manual. While not at the lightning-fast level of NotPetya, this operation was carefully planned and scheduled. In a couple of hours, their code was successfully delivered to most of its targets.[94]

[87] Researchers have deducted from the level of sophistication of the Crash Override malware and the relatively low impact it had that it must be a test-run for what could be destructive platform. This occurred merely six months prior to NotPetya: *see* WIRED, "Crash Override" and "The untold story of NotPetya".

[88] While the EU has developed sanction mechanisms in the event of hostile cyber operations, it still rests in its "toolbox": https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/; the most a government has done against Russia so far relates to the 2016 US elections meddling: E. Sanger, "Obama Strikes Back at Russia for Election Hacking", the New York Times (29 December 2016), available at: https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html; *see also* C. Miller, "What's Ukraine Doing To Combat Russian Cyberwarfare? 'Not Enough'", RFERL (07 March 2018), available at: https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html

[89] Despite a high-level of confidence from most security firms: WIRED, "Russia's infrastructure hacking teams"; https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/. Several States, notably part of the EU/NATO front, directly accused Russia as well: S. Alatalu, *NATO's Response to Cyberattacks,* Chaillot Papers (2018), pp. 98-100; the US as well: https://www.us-cert.gov/ncas/alerts/TA17-181A

[90] D. Denning, *Information Warfare and Security,* Addison-Wesley (1999), p. xiii

[91] Hansen & Nissenbaum, *Digital Disaster* (2009), p.1164

[92] WIRED, "The untold story of NotPetya"

[93] D. Bisson, "NotPetya: Timeline of a Ransomworm", Tripwire (28 June 2017), available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/; Politico, "How Ukraine became a test bed for cyberweaponry".

[94] WIRED, "Hack of Ukraine's power gird"

This supports the idea that, in the cyber realm, mere instants are needed to create long-lasting, heavy damage to multiple structures. We can compare "cyber outbreaks" to the sectors of pandemics or environmental security. While the former shares the feature of propagation but is much more containable; the latter connotes irreversible catastrophe, but fails to generate a feeling of urgency.[95] As already evoked, a parallel can also be drawn with nuclear security, which combines the irreversible and urgent qualities, but is not perceived as likely, or even possible in our contemporary international system.

Hypersecuritisation applied to cybersecurity should be understood as an inherent ability to create irreversible, large-scale damage in an instantaneous fashion. It counter-balances to the idea of constant insecurity, always in the background and is easily articulated with the cross-sector nature of cyber.

Combination

Rather than considering this factor as granting an "exceptional" status to a single (potential) threat, we should consider it together with the other structuring features of the cybersecurity sector as establishing a sector-specific *context* which establishes a pre-conditioned environment favourable to the securitisation process of a potential threat in the cyber realm. This is the first layer of a multi-level context influencing the following interactions, between actors, recipients, audience and the facilitating conditions that determine the acceptance of the speech act narrative.

This relates to the agent-structure relation developed in Chapter I, Section C. While Stritzel invokes a three-layered triangle, we should see this overarching interaction between the actors of security and their structural environment as encompassing the external factors influencing both the nature of the threat as well as the "positional power" between said actors.

Actors v. referent objects

We mentioned the little relevance of a static audience in the first chapter. Through a dynamic approach, the audience can gain significant agency when a portion – e.g.: civil society, or the media – attacks the securitising authority's discourse, sometimes to de-legitimise the actions it takes (which, in a democracy, can lead to discard the power in place and replace it, as we have seen with the recent elections in Ukraine).[96]

As previously supported, the State is not the sole holder of power in the process and other parts of society can generate meaning and trigger a securitisation attempt. Particularly relevant is the prominence of the private sector in the dialogue. Focused on an alternate referent object: the economy (in the form of its profits and revenues), it is also better equipped when it comes to defence against hostile actors in cyberspace.[97] For that reason, States increasingly give responsibility to the private sector, while the decision power and authority to undertake countermeasures remains largely with State agents.

[95] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1164

[96] *See e.g.:* RFERL, "What's Ukraine Doing To Combat Russian Cyberwarfare"

[97] The National Strategy, *The National Strategy to Secure Cyberspace,* Washington: White House (February 2003), p. 11.

If we observe how these elements create a sense of individual vulnerability with immediate consequences, it calls to reflect on an alternative approach regarding what constitutes a referent object of a threat, especially when we superpose the hypersecuritisation and everyday security practice notions, which collides instant possible threat with constant insecurity that can affect everyone, despite the implementation of preventive measures. It should not be understood as an opportunity to elevate the individual as a recipient on its own, but rather as encompassing a collective sense of insecurity at societal level.[98] Nonetheless, the power of every individual once he/she perceives its interest and safety threatened must not be underestimated and should encourage us to see it as a proper referent in and of itself, with a different set of priorities than the state or the private sector.

This entity one could qualify as *collective society* holds a particular status in that it can act as referent object, a targeted audience but also holds a nature of facilitating condition. This claim builds upon the critique against static elements and encouraging a more dynamic, flexible understanding of actors and referents.[99] Indeed, expanding the influential power of these actors as they react to the threat brought upon them strongly influence the impact of the speech act based on its trust in the securitising agent,[100] potentially reject it and even grasp a portion of the authority to undertake emergency action by discrediting the established power through new elections and other democratic processes.

Cyberspace enhances and accelerates this phenomenon, which Joseph Nye calls "power diffusion" via several of its key features: the challenge of attribution in cyberspace (*see infra*) and the exponential growth of the digital realm notably created new poles of governance and reduced the share of States' jurisdiction, which saw their authority capital drastically diminish in the cyber as well as the material realms. Indeed, following the Cold War and the end of bipolarity, not only did superpowers traded parts of their influence across the globe, notably with the emergence of international and regional organisations such as the UN, the European Union or NATO, to name the most prominent ones, but they also quickly lost their influence over multinational who grew especially powerful in the technology sector, with companies like Google or Facebook that dispose of unprecedented influence on the global market.[101] It sustains the idea that more actors hold a portion of (securitising) power, or influence.

On the other side of the coin, the individual itself constitutes a threat – or at least a form of facilitating conditions for securitising an event, even hypersecuritising it – in that it can render the larger structure of its firm vulnerable to malicious code. As said above, the large-scale attacks that took down the Ukrainian power grid can be traced back to spear-phishing operations where employees downloaded a virus-loaded file from an e-mail.[102] While the intention does not reside with the duped individual, the tricks put in place by hackers call for caution. Hansen and Nissenbaum made a comparison with the epidemics field in that "cyber

[98] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1165

[99] *See supra* Chapter I, Section C.

[100] T. Balzacq, *The Three Faces of Securitization: Political Agency, Audience and Context*, European Journal of International Relations vol. 11(2) (2005), pp. 40-41.

[101] *See* J. Nye, *Cyber Power*, Belfer Center for Science and International Affairs (May 2010)

[102] WIRED, "Hack of Ukraine's power gird"

insecurities are generated by individuals who behave irresponsibly thus compromising the health of the whole",[103] noting the semantic parallels between both sectors as our computers are "infected" with "viruses" and advice for "cyber-hygiene."[104]

This embodies a second shift of responsibility towards the users as they act as a security risk. However, unlike private corporations with abilities to protect their structures, mitigate and/or prevent damaging effects, unequipped citizens are largely defenceless as much as unaware while heavily reliant on a technology that goes far beyond their understanding. This could create a feeling of helplessness and carelessness that will increase the threat, while disrupting the discourse from the securitising agents and the ability to act influence its authority to implement exceptional measures. [105]

What must occur is a constellation of referents/actors that balance themselves via competing articulations of security. All actors – public, private and collective – must be able to be their own actors of securitisation all the while being capable to act as opposed audience in case of an unacceptable discourse. By mutually regulating their behaviours over cybersecurity issues, the burden of security and their relative, positional powers will adjust for the benefit of all.[106]

Lastly, we must highlight a special position amongst the influencing actors of cybersecurity: the expert community. Security experts, in a research capacity as part of firms tasked with investigating, analysing and addressing security issues such as the ones studied in this thesis, produce an esteemed opinion and their contributions to the definition of a threat is crucial. While they mostly belong to the private sector, it seems appropriate to grant them a special, hybrid status of securitising actors and educated audience.[107]

The importance of context in cyber securitisation

Regarding cyberspace in general, the idea of threat is omnipresent, as we previously labelled a "constant fleeting insecurity." This is can be seen simultaneously as a characterising the security dimension of the speech act and as an initial condition for the nature of the alleged threat. These two facilitating conditions taken together generate a context favourable for a securitising move, specific to the cyber sector.

We also previously addressed the grammar specific to cybersecurity and how its semantic theme facilitates its insertion in the security domain. It almost automatically categorises the speech act as a security discourse via its content only, or rather it brings the issue within a "linguistic structure" permanently covering the sector.[108] Rather than giving in to a static

[103] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1166; US *National Strategy to Secure Cyberspace* (2003), p. 11.

[104] Cyber hygiene is a set of behaviours and best practices to follow in order to remain resilient against and prevent computer security breaches, at individual, corporate or systemic levels. It can go from basic, yet crucial steps: https://www.csoonline.com/article/3310068/basic-cyber-hygiene-practices-that-go-a-long-way.html; to advanced methods, especially for large companies that require personnel training: *see e.g.* https://www.us-cert.gov/sites/default/files/resources/ncats/CyHy%20Sample%20Report_508C.pdf

[105] Hansen & Nissenbaum, *Digital Disaster* (2009), p. 1166

[106] *See ibid.*, pp. 1161-1163

[107] Among the firms relied on in this thesis are Dragos, FireEye, ESET, Kaspersky, etc.

[108] Stritzel, *Copenhagen and Beyond* (2007), pp. 366-367.

notion of defining speech act, we perceive a speech act within a pre-existing 'facilitating context' for discourse, that can be completed with an authoritative speech act that seek to confirm an event as exceeding the basic 'insecurity level' of the sector. Whether this will be accepted by the target audience will depend on other factors developed in this section, but it supports this thesis' claim that cybersecurity holds a special position amongst security sector.

If we couple this discursive pre-disposition to securitisation with the dynamic relations between actors and referent objects and the inherent characteristics of cyberspace in the security context – that is threat instantaneity, constant fleeting insecurity and cross-sector fluidity – we generate a unique framework, specific to the cybersecurity sector:

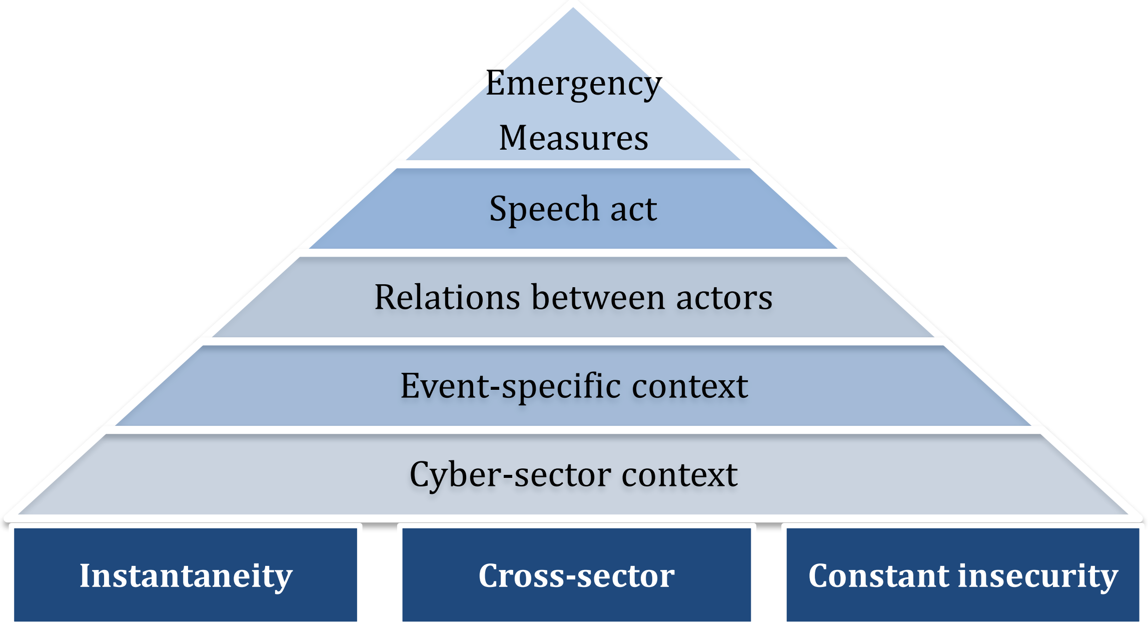

Figure 1 - The cyber-securitisation pyramid: a contextual approach

We observe how they build upon each other and while the three pillars and base level articulate a special base frame for the cybersecurity sector, the four top layers are applicable to any other field and issue, almost as is.

The second layer from the bottom, "event-specific context" relates to what we could rebrand "external determining factors", meaning how any situational or historic element could affect the chances of a successful securitising move. In the context of the attacks on Ukraine's infrastructures, the historic tensions with Russia and the recent geopolitical developments are one external factor, while the notorious behaviour of Russia in cyberspace is a sector-specific factor. Indeed, prior to the Ukrainian campaign, we shall keep in mind the cyber operations conducted against Estonia and Georgia in 2007 and 2008.[109] These not only share a strong semantic but also are geographically and historically linked in a fashion that enhances the perception of threat.

[109] P. Pernik, *Early Days of Cyberattacks: the Cases of Estonia, Georgia and Ukraine,* Chaillot Papers (2018), pp. 53-60.

Conclusion

The analysis performed in this thesis draws upon deeply rooted, extensive theoretical notions. The securitisation theory offers many prospects in analysing the security landscape in modern politics and much more could be said about its potential applications to emerging sectors of security studies.

Its rather open framework would furthermore allow drawing from adjacent theories such as the balance of threat, critical security studies or the actor-network theory to name a few. Nonetheless, we realised that the traditional approach of the Copenhagen School channels a certain amount of limitations that prevent its application to modern, complex issues.

The subject of cybersecurity is difficult to address, from its ambiguous nature, its highly technical dimension yet omnipresence in our everyday lives. In terms of security in the political theory context, the impact it brought to our vision of the world in just a few years was unparalleled. The pace at which technology still progresses today brings new opportunities but also significant challenges in terms of governance, security and humanity: artificial intelligence, drones, augmented individuals; these issues will also bring their share of ethical problems that will have to factor into our analysis of society. And all of them will be increasingly dependent on cybersecurity.

This justifies the need to thoroughly explore and research the theoretical frameworks that surround the security of our connected societies. We just very recently caught a glimpse of what a devastating cyberattack can be and how helpless our structures and authorities are in front of an unleashed malicious line of code.

In the narrow, specific context of this thesis, we developed a contextual and externalist approach to securitising events in cyberspace, defining threats that navigate across all traditional sectors and require a more dynamic exchange between influencing actors. The case study of Russian cyberattacks against Ukraine is the equivalent of a lab-environment sample testing. Indeed, the characteristics of this issue perfectly align for the purpose of applying a new framework, and the geopolitical context surrounding the issue provides a unique set of influencing factors.

Through this exercise, it was possible to design a revisited framework for the process of securitisation that takes more elements into account as well as considering the recent developments regarding the participants to the game of power politics. While this thesis' claims certainly merit to be tested against more real-life events and expanding towards additional theoretical currents, it gives a very distinct feature to the securitization theory that was lacking, in the opinion of this author, to the traditional approaches of Wæver, Buzan and de Wilde: flexibility.

While the approach developed throughout the second chapter was tailored for the cyber domain, we made sure to provide it with enough flexibility to recycle it and apply to other sector of security. In particular, the importance of context and the dynamic roles of the involved actors will bring a broader perspective upon complex issues without having to dismiss components in fear of overburdening the structure with multiple notions, a feature necessary in a rapidly evolving field, studying a rapidly changing world.

To conclude, one last element should be highlighted: security intrinsically looks towards the future but relies on past events to evolve. It is likely that we just entered a new era in terms of defining security in the cyber domain: the examples exploited in this thesis – BlackEnergy, Crash Override and NotPetya – are the first occurrences of what we should fear will become the new weapon of choice between nations at peace that wage war in the shadows.

We are currently witnessing a continuous challenge between three belligerent powers threatening and displaying their penetration abilities into each other's critical infrastructures. The US, Russia and Iran are accelerating the pace of cyber war, and we still lack a robust framework of analysis to anticipate the potential consequences on our societies.[110] Cyberspace is likely to be the battlefield of the 21st century, and while we might be safer from bombs and rockets, the entire network of societies share the same environment as these digital soldiers, and as we have seen, their weapons aim wide and do not always stick to their targets.

Efforts must be increased and collaboration enhanced across sectors, across political groups and across nations; because we are a click away from digital annihilation.

[110] *See* M. Schmitt, "U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?", Just Security (18 June 2019), available at: https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply/

Bibliography

Books

- Buzan B., *The United States and the Great Powers: World Politics in the Twenty-First Century*, Cambridge: Polity (2004)
- Buzan B. & Wæver O., *Regions and Powers: The Structure of International Security*, Cambridge University Press (2003)
- Buzan B., Wæver O. & de Wilde J., *Security: A New Framework for Analysis*, Lynne Rienner Publishers (1998)
- Denning D., *Information Warfare and Security*, Addison-Wesley (1999)
- Fierke K., *Critical Approaches to International Security*, Cambridge Polity Press (2007)
- Hay C., *Political Analysis: A Critical Introduction*, New York: Palgrave (2002)
- Jørgensen K., *International Relations Theory: A New Introduction*, New York: Palgrave Macmillan (2010)
- Kaplan F., *Dark Territory: the Secret History of Cyber War*, Simon and Schuster Paperbacks (2016)

Contributions in Academic Volumes

- Butler J., *Performativity's Social Magic*, *in* Schatzki T. & Natter W. (eds.) *The Social and Political Body*, New York: Guilford Press (1996), 29–47
- Buzan B., *The Timeless Wisdom of Realism?*, *in* Smith S., Booth K. & Zalewski M., (eds.), *International Theory: Positivism and Beyond*, Cambridge University Press (1996), 47-65
- Smith S., *The Contested Concept of Security*, *in* Booth K. (ed.), *Critical Security Studies and World Politics*, Lynne Rienner Publishers (2005), 27-62
- Wæver O., *Securitisation and Desecuritisation*, *in* Lipschutz R. (ed.) *On Security*, Columbia University Press (1995), 46–86
- Wæver O., *Identity, Communities and Foreign Policy*, *in* Hansen L. and Wæver O. (eds.), *European Integration and National Identity*, London: Routledge (2001), 20–50
- Wæver O., *The EU as a Security Actor: Reflections from a Pessimistic Constructivist on Post Sovereign Security Orders*, *in* Kelstrup M. & Williams M. (eds.) *International Relations Theory and the Politics of European Integration*, London: Routledge (2000), 250–294
- Yould R., *Beyond the American Fortress: Understanding Homeland Security in the Information Age*, *in* Latham R. (ed.), *Bombs and Bandwidth: The Emerging Relationship between Information Technology and Security*, New York: The New Press (2003), 74–98

Academic Articles

- Balzacq T., *The Three Faces of Securitization: Political Agency, Audience and Context*, European Journal of International Relations vol. 11(2) (2005), 171–201
- Booth K., *Security and Emancipation*, Review of International Relations, vol.17 (1991), 313-326
- Bubandt N., *Vernacular Security*, Security Dialogue, vol. 36 (3) (2005), 275–296

- Hansen L. & Nissenbaum H., *Digital Disaster, Cyber Security, and the Copenhagen School*, International Studies Quarterly, vol. 53 (2009), 1155-1175
- Krause K., *Critical Theory and Security Studies: The Research Programme of Critical Security Studies*, Cooperation and Conflict, vol. 33(3) (1998), 298-333
- Mastanduno M., *Preserving the Unipolar Moment: Realist Theories and U.S. Grand Strategy after the Cold War*, International Security, vol. 21(4) (1997), 49-88
- McDonald M., *Securitisation and the Construction of Security*, European Journal of International Relations, vol. 14(4) (2008), 563-587
- McSweeney B., *Identity and Security: Buzan and the Copenhagen School*, Review of International Studies, vol. 22 (1996), 81–93
- Nye J., *Cyber Power*, Belfer Center for Science and International Affairs (May 2010)
- Sterling-Folker J., *Realism and the Constructivist Challenge: Rejecting, Reconstructing, or Rereading*, International Studies Review, vol. 4(1) (2002), 73-97
- Stritzel H., *Towards a Theory of Securitisation: Copenhagen and Beyond*, European Journal of International Relations vol. 13(3) (2007), 357-383
- Walt S., *Alliance formation and the balance of world power*, International Security, vol. 9(4) (1985), 3-43
- Wang Y., *China's Response to the Unipolar World: The Strategic Logic of Peaceful Development*, Journal of Asian and African Studies, vol. 45(5) (2010), 554-567
- Wilkinson C., *The Copenhagen School on Tour in Kyrgyzstan: Is Securitisation Theory Useable outside Europe?*, Security Dialogue, Vol. 38 (1) (2007), 5-25
- Wyn R. W., *"Message in a Bottle"? Theory and Practice in Critical Security Studies*, Contemporary Security Policy, vol. 16 (1995), 299–319

Official Documents, Policies and Statements

- US, *National Policy on Telecommunications and Automated Information Systems Security*, National Security Decision Directive Number 145, Washington: White House (17 September 1984)
- US, Computer Science and Telecommunications Board (CSBT), *Computers at Risk: Safe Computing in the Information Age*, Report, Washington, DC: National Academy Press (1991)
- US, Computer Science and Telecommunications Board (CSBT), *Today and Tomorrow: Pay Now or Pay Later*, report, Washington, DC: National Academy Press (2002)
- US, The National Strategy, *The National Strategy to Secure Cyberspace*, Washington: White House (February 2003)
- US-CERT, Alert (TA17-181A) - Petya Ransomware (01 July 2017), available at: https://www.us-cert.gov/ncas/alerts/TA17-181A
- US, *National Cyber Strategy of the United States of America*, Washington: White House (September 2018)
- European Union, *Directive on security of network and information systems (NIS Directive)*, Policy Statement, available at: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
- Council of the EU, *Cyberattacks: EU ready to respond with a range of measures, including sanctions*, press release (19 June 2017), available at: https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

- Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London (23 May 2019), available at: https://www.nato.int/cps/en/natohq/opinions_166039.htm

Analysis Reports

- Connell M. & Vogler S., *Russia's Approach to Cyber Warfare*, Report, CAN (March 2017)
- Geers K. (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, Report, NATO CCDCOE (2015)
- Giles K., *NATO Handbook of Russian Information Warfare*, Monograph, NATO Defence College (November 2016)
- Langner R., *To Kill a Centrifuge*, Report, The Langner Group (November 2013), available at: https://www.langner.com/to-kill-a-centrifuge/
- Popescu N & Secrieru S. (eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies*, EU Institute for Security Studies Chaillot Papers n° 148 (October 2018)

Media Resources

- Bisson D., "NotPetya: Timeline of a Ransomworm", Tripwire (28 June 2017), available at: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/
- Cerulus L., "How Ukraine became a test bed for cyberweaponry", Politico (14 February 2019), available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/?fbclid=IwAR2YvS7Cq6zrcObPELejDyWBsJtF3MAXxy3PzgwI0ZcbDW9SGkEtC5vZyas
- Fruhlinger J., "Petya ransomware and NotPetya malware: What you need to know now", CSO Online (17 October 2017), available at: https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html
- Giandomenico A., "Basic Cyber Hygiene Practices That Go a Long Way", CSO Online (01 October 2018), available at: https://www.csoonline.com/article/3310068/basic-cyber-hygiene-practices-that-go-a-long-way.html
- Greenberg A., "Your guide to Russia's infrastructure hacking teams", WIRED (12 July 2017), available at: https://www.wired.com/story/russian-hacking-teams-infrastructure/
- Greenberg A., "'Crash Override': the malware that took down a power grid", WIRED (12 June 2017), available at: https://www.wired.com/story/crash-override-malware/
- Greenberg A., "The untold story of NotPetya, the most devastating cyberattack in history", WIRED (22 August 2018), available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
- Hay Newma L., "The leaked NSA tool that hacked the world", WIRED (07 March 2018), available at: https://www.wired.com/story/eternalblue-leaked-nsa-spy-tool-hacked-world/
- Miller C., "What's Ukraine Doing To Combat Russian Cyberwarfare? 'Not Enough'", RFERL (07 March 2018), available at:

https://www.rferl.org/a/ukraine-struggles-cyberdefense-russia-expands-testing-ground/29085277.html

- Park D., Summers J. & Walstrom M., "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks", JSIS (11 October 2017), available at: https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/#_ftn12
- Sanger E., "Obama Strikes Back at Russia for Election Hacking", the New York Times (29 December 2016), available at: https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html
- Schmitt M., "U.S. Cyber Command, Russia and Critical Infrastructure: What Norms and Laws Apply?", Just Security (18 June 2019), available at: https://www.justsecurity.org/64614/u-s-cyber-command-russia-and-critical-infrastructure-what-norms-and-laws-apply/
- Yuang Y., "The Great Firewall of China: Web of Control", Financial Times (12 March 2019), available at: https://www.ft.com/content/e19b3022-40eb-11e9-9bee-efab61506f44.
- Zetter K., "Inside the cunning, unprecedented hack of Ukraine's power grid", WIRED (03 March 2016), available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
- X., "Privacy and Surveillance Post-9/11", American Bar Association (30 June 2017), available at: https://www.americanbar.org/groups/crsj/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11/
- X., "Ukraine election: Comedian Zelensky wins presidency by landslide", BBC (22 April 2019), available at: https://www.bbc.com/news/world-europe-48007487

Technical resources

- Cherepanov A. & Lipovsky R., "Industroyer: Biggest threat to industrial control systems since Stuxnet", Welivesecurity (12 June 2017), available at: https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/
- Cherepanov A. & Lipovsky R., "New TeleBots backdoor: First evidence linking Industroyer to NotPetya", Welivesecurity (11 October 2018), available at: https://www.welivesecurity.com/2018/10/11/new-telebots-backdoor-linking-industroyer-notpetya/.
- Hultquist J., "Sandworm Team and the Ukrainian Power Authority Attacks", FireEye (07 January 2016), available at: https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
- Lee R., "CRASHOVERRIDE: Analyzing the Malware that Attacks Power Grids", Dragos, available at: https://dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/
- Lipovsky R., "Seven years after Stuxnet: Industrial systems security once again in the spotlight", Welivesecurity (16 June 2017), available at:

https://www.welivesecurity.com/2017/06/16/seven-years-stuxnet-industrial-systems-security-spotlight/

- Wilhoit K., "KillDisk and BlackEnergy Are Not Just Energy Sector Threats", TrendLabs Security Intelligence Blog (16 February 2016), available at: http://blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats
- Dragos, "Industrial control system threats", Report (01 March 2018), available at: https://dragos.com/wp-content/uploads/2017-Review-Industrial-Control-System-Threats.pdf
- Kaspersky, "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from within", available at: https://www.kaspersky.com/blog/the-human-factor-in-it-security/
- Search Security, Distributed Denial of Service Attack: Definition, available at: https://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack
- Search Security, Ransomware: Definition, available at: https://searchsecurity.techtarget.com/definition/ransomware
- Search Security, Malware: Definition, available at: https://searchsecurity.techtarget.com/definition/malware

All online sources (websites) have been last visited on 5th July 2019