Swedish Defence University

Managing Crises Level 2: The Cyber World
Delving into the Unknown

Maria Foteini Prevezianou

Swedish Defence University
Master's Programme in Politics and War
2017-2018

Supervisor: Professor Magnus Ekengren

Word Count: 12.401

Table of Contents

Abstract

The present paper attempts to delve into the underexplored field of cyber crisis management, by initiating an academic problematization on crisis conceptualization and crisis management theory. It uses the theoretical framework of transboundary crisis management in order to examine two different major cyber attacks, the 2017 WannaCry ransomware attack and the 2016 hacking of the DNC, and answer an empirical puzzle: why are these cases not characterized as crises even though they fit already existing definitions? The study concludes that this grey area in terminology is generated by an academic reluctance to delve into the cyber domain and consequently by using old concepts to explain new threats. Moreover, it contributes to the theory of transboundary crisis management by shedding light on certain characteristics of cyber crises which were previously overlooked.

Introduction

> *"Just as we're all connected like never before, we have to work together like never before, both to seize opportunities but also meet the challenges of this information age. It's one of the great paradoxes of our time that the very technologies that empower us to do great good can also be used to undermine us and inflict great harm"*.[1]
>
> *Barack Obama (2015, February 13)*

Attempting to talk to security and crisis management scholars about cyber-related issues is like asking a toddler to ride a bike. It seems exciting, they want to do it, but they have a fear of falling. Even though they realize it is a very "hot" field in today's new threat landscape that brings new research challenges to the table, they seem reluctant to touch upon it and often believe that the cyber domain is the responsibility of IT experts sitting in front of computers and typing ones and zeros. But what happens when a crisis actually hits?

While it is true that IT experts are a crucial part of the cybersecurity field, it is also true that cyberspace can have multiple dimensions as it falls within multiple domains. That automatically makes it relevant to the study of security and crises and pushes academics to broaden their horizons to new areas of research. The study of the crisis concept has always been a fascinating and intriguing research challenge. Adding

[1] From President Obama's speech at Stanford University: Guion, 2015.

the cyber element to that will open the door to a new world and serve as a point of departure for the examination of the new guises of the crisis concept.

Consequently, the present paper attempts to initiate an academic problematization on the issue of cyber crises, by going beyond the "ones and zeros" and build the necessary bridge between the technical aspect and the crisis management aspect. The motive behind this choice was an interesting observation. Several researchers have had a significant contribution to the field of cybersecurity, and certain cybersecurity organizations, such as the European Union Agency for Network and Information Security (ENISA), or national cybersecurity centres have published a significant number of reports and cybersecurity strategies. At the same time, international relations scholars have also been highly productive in the study of cyber warfare and its impact in the field. On the contrary, even though we live in the era of interconnectedness, cyber crisis management is an alarmingly underexplored field of research. Taking this observation as a point of departure, the present paper attempts to delve into the deep waters of the cyber world and examine its interaction with the field of crisis management.

Defining the Research Problem

For security and crisis management scholars, the concept of crisis itself has been the subject of rigorous academic discourse. Entering an era of new transboundary threats, unprecedented in nature, inevitably intensified the already existing academic turmoil and put pressure on academics to reconsider their theoretical frameworks and policy makers to improve their reflexes in the face of the unknown. The vigorous growth of the cyber domain is a significant element of the new threat landscape, as it constitutes a new hotbed of potential crises that neither policy makers nor academics had dealt with before, and gave rise to a new subfield, that of cyber crisis management.

Despite the initial hesitance to delve into the unknown, there have been significant academic efforts to map the "cyber Wild West"[2] and the policy makers' mobilization towards the protection of the digital world is indeed worth noting, even though the level of cybersecurity among nations and organizations still varies

[2] For an example of such an effort, see Backman's analysis on the institutionalization of cybersecurity management at the EU level: Backman, 2016.

significantly. However, when moving from theory to practice and after examining the empirics, an interesting observation arises; determining whether a cyber attack constitutes a crisis or not is still a grey area in the field of cyber crisis management and certain terminological barriers are still a source of confusion.[3] Bearing these factors in mind, the present paper attempts to delve into the intriguing field of crisis management and examine if and in what ways this field is challenged in a relatively new area, the cyber world.

Political science researchers have been stressing the need to justify new research by taking "real-world problems" as a point of departure. [4] After identifying the problem, it is necessary to use problematization as a tool to challenge already existing theoretical assumptions and produce more influential theories, instead of merely searching for gaps in the literature.[5] Bearing these research guidelines in mind, it could be argued that crises are probably the ultimate real-world problem. They are an inherent feature of society, which has been keeping primarily decision makers and secondarily academics alert. Even if it might not be obvious at first sight, all concepts of security, or even the new "hot" term of resilience, have been built upon the inherent sense of fear, both individual and societal, of new threats that arise and how they can be managed in such a way so as not to cause severe disturbances in the proper functioning of society. In this context, there is no other field that would be more adequate for research than that of crisis theory and management.

The present paper takes a closer look at the cyber world and explores in what way this new domain brings in new dimensions to what was already known and established about crises. Thousands of pages have been written in an attempt to conceptualize crises and evaluate the crisis management mechanisms' response to them. However, it could be argued that the academic community still seems reluctant to touch upon the issue of cyber crises, with experts mostly speaking of cyber attacks or cyber incidents. It is an undeniable fact that the cyber domain takes over more and more aspects of our daily lives, which does not come as a surprise, considering the rapid technological development in today's world. At the same time, statistics show a significant rise in the number of cyber attacks, which will have a greater impact on people's life the more interconnected we get. Only in September 2018, cyber attacks

[3] For an analysis of issues regarding terminology, see: Trimintzios et al., 2014, p. 24.
[4] Gustafsson and Hagström, 2017, p. 4.
[5] Alvesson and Sandberg, 2011.

reached the number of 106 events, against the 80 of August,[6] while the academic community is still struggling to come to an understanding of what a cyber crisis really is. It will not be long until a major cyber crisis hits, and crisis managers are dumbfounded by its escalation potential.

This, however, does not mean that all cyber attacks fall within the crisis concept. A vast number of cyber incidents have been handled successfully with ordinary management mechanisms and both the private and public sector have been dealing with cyber threats since the emergence of the cyber domain. However, as the following chapters attempt to prove, there are certain cases which generate academic concern as to whether or not we have a clear understanding of what we are called upon to encounter. The following paragraphs constitute an attempt to clearly define the source of the research problem and its academic contribution.

Empirical Puzzle

A well-defined problem is the alpha and omega of every research project. Conducting a study without a clear understanding of its purpose, contribution and connection with the empirics is like driving a car with no clear destination: a meaningless ride. Drawing from Shapiro, who has been arguing for "problem-driven over method-driven approaches to the study of politics",[7] it is vital to pinpoint the elements that are necessary for the construction of the present research problem.

In order to justify the need for new research, Gustafsson and Hagström recommend the construction of a research puzzle based on a "Why x despite y" formula.[8] Why do we observe a certain empirical pattern occurring (x), even though theory suggests otherwise (y)? Even though cyber security and crisis management is a newly emergent field, there have been efforts to define the concept of a cyber crisis and how it is differentiated from smaller scale incidents in official strategy documents, academic literature and best practice reports.[9] However, when studying several cyber attacks, an interesting observation arises; certain cases that do present all the characteristics required in order to be categorized as crises, are usually described as attacks. This creates a grey area in the way we define such events and constitutes a source of confusion. Terminological grey areas can be more "dangerous"

[6] Passeri, 2018.

[7] Shapiro, 2002, p. 598.

[8] Gustafsson and Hagström, 2017, p. 6.

[9] For instance, see: Trimintzios et al., 2014.

than expected. The establishment of certain definitions, constructed by the academic world, is not cut off from the real world. Definitions are not used by academics just for the sake of research. They are inextricably linked to the activation of certain mechanisms. By failing to determine whether a case in the cyber domain is a crisis or not, we simultaneously fail to activate the necessary mechanisms to cope with it. At the same time, overreacting to a regular incident and classifying it in the crisis category can also have a negative effect as it could cause societal distress and political upheaval.

As a consequence, this empirical puzzle serves as a great opportunity to delve into the crisis concept and examine its dynamics and potential challenges in the cyber domain. Which is the root cause of this puzzle? What research questions could be drawn from it and how can the answers to those questions broaden our crisis perspective? What is this study a case of?

Research Questions drawn from the Puzzle

Drawing from the empirical puzzle described above, the present paper aspires to give an answer to the following research questions:

1. Is the traditional perception of a crisis still valid in this new threat landscape and are traditional crisis concepts sufficient in the cyber domain?

2. How can the examination of certain major cyber attacks, which still remain underexplored, contribute to a better understanding of the new research area of transboundary crises? What more do the distinctive features of these specific cases have to add to the academic debate on crises?

Purpose: Why is it important?

The relationship between academia and policy making has always been one of cross-fertilisation. While the former collects and analyzes data and draws conclusions which could prove vital for decision makers, the latter is responsible for shaping reality in such a way that urges academia to constantly reconsider its analytical tools and frameworks so as to keep up with real-world change. The development of the cyber domain is no exception to the rule, as this new field puts pressure on decision-makers to ensure security in cyberspace, while statistics speak of a rise in cyber attacks, which puts the need to secure cyberspace higher in the political agenda than in the past. This in turn challenges academics' conventional theories on security and crisis management and highlights the need to add the cyber element in academic research.

Consequently, the present study serves a dual purpose:

(a) To enhance our understanding (how-question) and raise awareness:

How are cyber attacks changing the already existing threat landscape? How can they change our crisis perspective and in what way will this change affect crisis management models? A lack of understanding of the new threats will result in us managing them the same way as other conventional threats and, thus, follow a "one size fits all" logic. Non-technicians need to familiarize themselves with how to handle the new challenges that arise. Moreover, the terminological ambiguity makes it harder to recognize a cyber crisis as such. This could be detrimental to cyber security, as it makes us underestimate the potential consequences of a cyber crisis spilling over into the real world.

(b) to explain (why-question):

Why do we observe this puzzle? Is there a gap in previous literature or are there factors that have been overlooked because scholars have failed to touch upon them? Is there a need to reconsider already existing theoretical frameworks or add new elements to them?

Therefore, the present paper has a dual research objective;[10] it moves from theory testing (traditional crisis management and crisis concepts) to theory building (new crisis characteristics which will add a new dimension to the theory of the transboundary crisis). By critically examining the cases and gaining insight into the issue, academics and policy makers can improve, at least to some extent, their ability to predict the nature of future crises and be proactive instead of reactive to threats.

[10] For a methodological discussion on research objectives, see: George and Bennett, 2005, p. 75.

Methodology

Research Design: Choosing which methodological path to follow

The research problem of this study lies on the argument that certain major cyber attacks could be characterized as crises, but there is still an academic reluctance to delve into the issue and it is usually preferred to use the more “convenient” term of cyber attacks. It also argues that certain cases are indeed cases of transboundary crisis management and should be studied further in order to add new aspects to the transboundary crisis framework. Attempting to test this argument, the present paper chooses to examine two different cases that both serve the same purpose: (a) the 2017 Wannacry ransomware attack and (b) the cyber attacks (hacking) on the Democratic National Committee (DNC) during the 2016 US Elections.

The selection of cases is a crucial step in order to design a good research strategy and achieve the study’s objectives.[11] The choice of these two cases is not coincidental. Both attacks take place in cyberspace and are transboundary in nature. This puts them under the same category, which helps the researcher draw useful conclusions. However, they have significant differences:

1. The Wannacry was a worldwide cyberattack that spread rapidly across 150 countries, whereas the cyber attacks on the DNC affected the US and Russia, due to its alleged involvement in the attack. Even though they are both transboundary in nature, the number of countries affected is different. This serves the purpose of the paper because, despite this difference, we can still observe certain common patterns that differentiate a cyber crisis from a conventional one and prove that these attacks can indeed be characterized as cyber crises and not simply attacks.

2. A more technical difference is that the Wannacry is a ransomware attack whereas the DNC hacking is an attack that involves data breach and email leaks. This makes the conclusions reached in the study more generalizable as they can apply to different types of attacks instead of just one, if the researcher had chosen to conduct a single case study.

3. Even though both attacks are multi-dimensional, in the sense that they can have an impact on multiple sectors, we could argue that the DNC hacking has a more political dimension – it affects the state’s legitimacy and institutional integrity and

[11] George and Bennett, 2005, p.83.

initiates discussions on democratic failure – whereas the Wannacry caused financial damage and also had a severe impact on critical infrastructure, such as hospitals, which could potentially have a tremendous societal impact, in case lives were lost. This also has an impact on the legitimacy of public institutions but in a more indirect way, as it was not the primary aim of the attackers. This difference shows how the conclusions reached can apply to multiple dimensions of a potential cyber crisis and not only a specific type of attack. A cyber crisis is, for instance, not only connected to an attack with strictly political goals or one that only causes damage on critical infrastructure.

However, this paper is not a comparative study. The conclusions reached are not drawn from the comparison between the two cases. It follows a multiple case study research design. This design was chosen as it offers the theory greater generalizability and higher inferential leverage, compared to a single case study. Choosing a single case study would be very beneficial in terms of delving deep into the characteristics of a specific case, but this would run the risk of the conclusions being simply an exception to the rule, i.e. already existing literature, whereas studying two cases – or even more depending on space limitations – contributes to the formation of patterns. These patterns are necessary in order to examine whether these cases have anything new to add to the literature. This study will, thus, look into two cases of major cyber attacks and draw conclusions that could prove valuable for the theoretical framework of transboundary crisis management.

These two cases are not the only cyber attacks to date. However, they were chosen because of the unprecedented scale and speed of expansion (Wannacry) and the direct impact on the legitimacy of public institutions (DNC hacking). Due to space limitations, the selection of more than two cases would not be possible. Other cases such as the Stuxnet computer worm attack on Iran’s nuclear facilities or the 2015 Ukrainian power grid cyberattack could serve as alternatives but they run the risk of being considered closer to theories on cyber warfare, which is beyond the scope of this study. Especially the latter took place during an ongoing Russian-Ukrainian War. In this paper it was preferred to study cases that are not directly connected to cyber warfare. Moreover, the 2007 Estonian cyber attacks have already been the subject of academic analysis and they are already characterized as a crisis.[12] Therefore, they could not be connected to the study's puzzle.

Finally, the research design chosen will move inductively from observing certain patterns and dynamics after examining the empirics, to adding new elements to the theory of transboundary crisis management.

Strategy of Data Collection

The necessary data for this study were collected by already existing academic literature (books, academic papers) on issues regarding crisis management, which will be reinforced by official reports from public institutions as well as private cybersecurity companies. For the examination of the empirics the study will be based on media articles due to a lack of previous studies on the issue, as well as a high level of secrecy when it comes to sensitive national security matters.

Moreover, in an attempt to reinforce the paper's argument, interviews were also included in the research process. As Steinar points out, "if you want to know how people understand their world and their life, why not talk with them?"[13] In particular, three cybersecurity experts, two from the private and one from the public sector were asked to offer their insight on the issue through a semi-structured interview that would allow for a more fruitful discussion and allow the interviewees to refer to issues that might not have been planned to be included. The interviewees will remain anonymous as anonymity allowed them to freely express their views. All three of them were based in Sweden. Interviewing experts from different countries and institutions would better serve the purpose of the paper but it was not possible due to unavailability. However, Sweden is one of the most interconnected countries in the world, which means that the experts interviewed are highly experienced and qualified in the field of cybersecurity.

Data Analysis

The present paper will use a qualitative textual analysis as a method of interpreting the available material described above, combined with a discourse analysis of the interviewees' answers.[14] The discourse analysis will shed light on certain patterns that

[12] Herzog, 2011.
[13] Steinar, 1996.
[14] Bergström and Boréus, 2017.

emerge when comparing the responses of different interviewees to the same questions, which would have been overlooked by simply conducting content analysis.

Limitations

The study does not come without certain limitations that need to be addressed. First and foremost, due to the lack of technical expertise, the technical aspect of the attacks will not be thoroughly analyzed and specialized technical details that could be hard for readers to grasp will not be included, as this would also go beyond the scope of the study. Instead, emphasis will be placed upon crisis management theory and issues related to the crisis concept. Technical details would be the responsibility of an IT expert and not a security studies' researcher, even though these details could prove highly beneficial when it comes to achieving a better understanding of the cyber domain.

Moreover, due to space limitations, the study cannot focus on each and every phase of crisis management or examine the effectiveness of crisis management mechanisms in these two cases (e.g. a separate analysis on sense-making, decision-making, attribution issues, etc.) for two reasons: (a) considering the complexity of the attacks examined and the vast number of countries involved, it would take a separate research paper to study if cyber crisis management mechanisms were effective or not, (b) the purpose of this paper is not to map institutional responses, as this has already been the subject of various studies. This paper aspires to have a more academic contribution to the concept of crisis and add new elements to the field of crisis management by adding the cyber dimension and its challenges.

Another issue that needs to be pointed out is the sensitivity of the cybersecurity domain for nation states as well as private companies, which means that certain information is classified and, thus, inaccessible to researchers, at least for the time being. There is also a considerable lack of material. Cyber crisis management is a new field which seems hard to grasp and the available academic material is not as much as in general crisis management. However, this serves the paper's purpose and makes its contribution highly significant for the academic world. Furthermore, it needs to be noted that both of the cases chosen are very recent which could justify the lack of previous research.

Last but not least, a reasonable question regarding the theoretical framework could arise; is crisis management really a theory? Or is it a research field? Crisis management is indeed a field, but taking a closer look at the academic effort within the field, one can observe the emergence of a significant academic debate regarding the nature of crises and subsequently how they can be managed. The following chapters constitute an attempt to answer this question by demonstrating the debate as well as add the cyber element to the debate.

Going Back to the Roots: Previous Literature

Traditional Crisis Management Theory and Crisis Concepts

Studying about crises is not a new research trend. Scholars have been problematizing on the issue for a very long time. Crises and disasters, either natural or man-made, and the way they are or should be handled by the public administration and the already existing crisis management mechanisms have been the subject of a long-standing academic debate. This does not come as a surprise, considering that each and every crisis that occurs brings to light new characteristics and new challenges, which put pressure on the policy makers' management capabilities and consequently fuel academic discourse. Ranging from pandemics and large-scale natural disasters to terrorist attacks, financial crises and critical infrastructure failures, the world has faced a vast number of crises and will probably continue to do so.

Traditionally, the concept of crisis has been connected to events out of the ordinary, which cause a serious disturbance to the smooth functioning of a system and cannot be handled with ordinary means. A crisis does not refer to any type of disturbance. Instead, it is described as "a serious threat to the basic structures or the fundamental values and norms of a system", which is characterized by a very high level of uncertainty, ambiguity and urgency, has a severe societal impact and pushes for critical decision making.[15] Due to the unprecedented nature of the threat, it constitutes a crash test for decision makers and organizational structures, which are being pushed to their limits. In this context, researchers have also discussed the issue of legitimacy and its role in conceptualizing crises, as a crisis also occurs "when the

[15] Rosenthan, Charles and t' Hart, 1989, p. 10.

institutional structure of a social system experiences a relatively strong decline in legitimacy as its central service functions are impaired or suffer from overload".[16]

The characteristics mentioned above demonstrate some core differences between a crisis and a regular incident or malfunction which can be handled with already existing incident mechanisms and could be considered "business as usual". On the contrary, as brilliantly pointed out by Rosenthal and Pijnenburg, crises "do forward the awkward dimension of 'un-ness': unexpected, unscheduled, unplanned, unprecedented and definitely unpleasant".[17] This "unpleasant" event is also a major driver for change, as it reveals certain structural deficiencies; the lessons learnt question the management capacity of entire policy sectors and even call for a change in already existing institutional arrangements.[18]

When the academic community first touched upon the crisis problematique, it mostly focused on urgent and unexpected events that require a fast response in order to minimize their societal impact, as well as the type of coping capacities national governments should develop in order to ensure that both society and state will bounce back from the crisis turbulence. Globalization and interconnectedness were at the time issues that did not "keep researchers up at night", as the core research challenge was the national – unilateral level of response, which was then considered sufficient. Considering that the referent object of security studies, which are also intrinsically linked to crisis management, has traditionally been the nation state – at least before the shift towards the individual as the new referent object – crisis conceptualization was bound to follow the same theoretical path.[19]

In this context, crisis management researchers have written extensively on how individuals, decision makers and institutions respond to such events and the dynamics behind their responses, as well as the challenges in every stage of an unfolding crisis. The stages are usually categorized in a before (crisis prevention and preparation), during (crisis response and coping) and after (crisis recovery and aftermath) phase, with the crisis coping phase to be the most challenging. In an attempt to break this phase down to analytical steps, researchers have identified another set of sub-phases, such as (a) sense-making, (b) meaning-making, (c)

[16] Boin, 2004, p. 168.
[17] Rosenthal and Pijnenburg, 1991, p. 1.
[18] For a thorough analysis of the concept of "institutional crisis", see: Ansell, Boin and Kuipers, 2016, as well as Boin and t' Hart, 2000.
[19] Boin, Ekengren and Rhinard, 2014.

decision-making, (d) termination and (e) learning and reform.[20] However, public bureaucracies were, at the time, not built in such a way so as to produce “highly dynamic responses”[21] and the crisis management capacity was still far from being institutionalized.[22] Consequently, academics focused more on what we could call ‘traditional’ and more ‘localized’ crises.

Taking a Step Forward: Present Theoretical Framework

A new chapter in the book of crises was written when the ‘modern’ or – to use a more common term – ‘transboundary’ crisis emerged, and, suddenly and unexpectedly, former crisis concepts proved insufficient to meet the challenges of the new threat landscape. From a focus on the nation-state and more localized responses to traditional crises, decision makers and academics were faced with threats that could not be halted by state borders, as a result of globalization and, consequently, an increased level of interconnectedness. Terrorist attacks, financial crises spilling over from one country to another, pandemics, cyber attacks and unprecedented natural disasters are only a few of the examples that shocked the crisis management community and initiated an academic debate on the need to reconsider the already existing nature of crises and their challenges.

Boin, who has been writing on crisis management for years with a major contribution in the field, has been systematically addressing the need to identify this newly emergent crisis concept. As he accurately describes, the modern crisis cannot be contained by national borders as “it thrives on fragmentation and variety. Its complexity defies governmental efforts to understand its causes, pathways, and potential remedies. The modern crisis does not confine itself to a particular policy area (say health or energy); it jumps from one field to the other, unearthing issues and recombining them into unforeseen megathreats. The modern crisis is not boxed in by set dates that mark a clear beginning and ending; it is an embedded vulnerability that emerges, fades, mutates, and strikes again”.[23] And as the complexity of social systems

[20] Boin et al., 2005.
[21] Ansell et al., 2010.
[22] Boin, 2004.
[23] Boin, 2004, p. 166.

continues to increase, even the slightest disruption is enough to lead to rapid escalation, and create a cascading effect.[24]

It was then more than obvious that the academic community needed to broaden the research agenda so as to formulate new theoretical perspectives that will effectively address these new challenges and enhance society's response capacity.[25] Even though our capacity to cope with traditional crises has improved significantly, there is a shift in the shape and dynamics of crises which calls for academic exploration of this "terra incognita",[26] and the creation of a common crisis language.[27]

Indeed, there has been a significant academic effort to delve into the unknown waters of transboundary crises and scholars of the field have identified certain common patterns. The following paragraphs constitute an attempt to summarize the basic features of modern – transboundary crises as indicated by researchers of the field, in order to determine the theoretical framework used in this study:[28]

1. *No boundaries:*

As already indicated by the term, a core feature of today's crises is their ability to transcend boundaries, not only geographical, but also political and functional.[29] This means that they can surpass national or even regional crisis management capacities, political jurisdictions, as well as life sustaining systems and infrastructures, and thus bear a "dynamic of systemic implosions".[30]

2. *No beginning and no end – beyond the traditional time sequence:*

The modern crisis challenges traditional time sequence and its effects are not necessarily identified at the same time period as the crisis explosion but might be felt "years down the road",[31] which further challenges the sense making phase of a crisis.

[24] For more on how complex systems make failures inevitable, see: Perrow, 1999.
[25] Boin, 2005.
[26] Boin, 2009.
[27] Boin, 2004.
[28] Due to space limitations, the analysis will not be thorough, as the purpose of this study is mainly to examine how these features emerge in cyberspace.
[29] Ansell et al., 2010, p. 196.
[30] Lagadec, 2009.
[31] Boin, 2009, p. 368.

3. *Crises of legitimacy:*

In contrast with traditional crises, the transboundary crisis might not necessarily result in loss of lives or pose a direct threat to human lives. However, they can cause significant, or maybe even greater, damage by undermining the legitimacy of the state and public institutions. As explained by Boin, “the currency of the modern crisis is not solely, or even primarily, expressed in the number of dead and wounded; it also attacks the legitimacy of the state, undermining its crisis management capacity”.[32]

4. *Greater escalatory and damage potential due to complexity:*

Deeply intertwined and complex system expose societies to severe threats, as only one vulnerability is enough to open the door to a crisis with great escalatory potential.[33]

5. *Authority vacuum:*

Since modern crises hit highly complex systems, questions regarding who owns the crisis and who has the authority to deal with it will unavoidably be raised.[34]

In a 2018 article, Arjen Boin explains how we are still unprepared for this type of crisis and addresses the need to rethink already existing crisis management arrangements. He concludes by setting a research challenge: “It is important to study the different guises in which the Transboundary Crisis comes, which allow for classification. [...] By studying cases of actual crises and near misses, we should be able to enhance our understanding of the Transboundary Crisis”.[35] This means that there is still an academic need for research on this area and examination of different aspects of the phenomenon.

As a consequence, the present study picks up the gauntlet and uses the theoretical framework of Transboundary Crisis Management as a point of departure, but moves one step further and examines its dynamics in the cyber domain. The cases analyzed will add new elements to already existing research and, at the same time, they will also shed light on the underexplored field of cyber crisis management.

[32] Boin, 2004, p. 166.
[33] Boin, 2018.
[34] Boin, 2009, p. 368.
[35] Boin, 2018, p. 6.

From Theory to Reality: Examination of the Empirics

Case 1: 2017 WannaCry Ransomware Attack

The Chronicle of the Attack: How did it unfold?

Considering that the WannaCry ransomware cryptoworm[36] infected hundreds of thousands of computers all over the world within a day, it could be argued that it managed to justify its name. The following paragraphs constitute an attempt to simplify the technical jargon and come to an understanding of the way the attack spread, its magnitude and impact.

Ransomware is a type of malicious software which is designed to prevent or limit users from accessing their systems. In order to regain access and control of their data, it demands that they pay a ransom by a set deadline, using online payment methods.[37] In particular, the WannaCry is a ransomware cryptowarm, which means that (a) it restricts access by encrypting users' data and (b) it can replicate and spread itself within networks without user interaction. It targets the Microsoft Windows Operating System, encrypts 176 different file types and asks users to pay a US$300 ransom in the bitcoin cryptocurrency. It warns that the amount will be doubled after three days and claims the encrypted files will be deleted after seven days if the payment is not made.[38] However, paying the ransom does not guarantee users that their files will be decrypted. But how did everything start? Which was the initiating point of the WannaCry attack and how did it escalate to the point of being a global threat?

The root of the problem was a security vulnerability in Microsoft Window's operating system, known as "EternalBlue". It is believed that the US National Security Agency (NSA) had discovered this vulnerability and, instead of reporting it to Microsoft, developed an exploit to weaponize it and use it as a new hacking tool for its own offensive purposes.[39] This tool exploits faults in a Windows Protocol called "Server Message Block" and remotely infects vulnerable computers. When Microsoft became aware of the vulnerability, it issued a security bulletin in March 2017 which

[36] Also known as WannaCrypt / WanaCrypt0r / WCrypt / WCRY: ENISA, 2017.

[37] For more details, see: Europol, n.d.

[38] Symantec, 2017b.

[39] The NSA has not confirmed that it created EternalBlue, but it has been anonymously revealed by former NSA officials: Nakashima and Timberg, 2017.

included security updates – also known as patches – for all Windows versions.[40] However, an alarmingly large number of Windows users, including companies and organizations, neglected to install the updates. In April 2017, a hacker group called The Shadow Brokers, which had been active since summer 2016, leaked several hacking tools, which were allegedly developed by the NSA, including EternalBlue. The leak is of utmost importance for what was about to follow, as it made these cyber weapons available and revealed critical software vulnerabilities to anyone wishing to exploit them.

As the subsequent course of events revealed, this vulnerability was enough to facilitate the outburst of a massive ransomware explosion. On Friday 12th May 2017, the EternalBlue vulnerability opened the door to the WannaCry ransomware cryptowarm. Although the way in which the first computer was infected is not yet determined, it is believed that this attack did not follow the common spreading method of phishing e-mails, but, according to ENISA, the worm remotely exploited vulnerable systems through Internet scanning and replicated itself so as to spread from one vulnerable computer to another.[41] This also explains the unprecedented speed of the attack's expansion. According to Europol, after the initial infection, the attack managed to hit over 200,000 victims in at least 150 countries within a day,[42] and the number was expected to grow the following week. Considering that the attack targeted all users that had not installed Microsoft's security patches two months prior to the attack, the vast number of victims is indeed alarming and a source of problematization as to how negligence can open the door to unimaginable threats.

At this point, a reasonable question could arise; why has this caused so much concern? Does this attack have anything to do with the real world or is it simply a "cyber issue", disconnected from our everyday lives? For all those unfamiliar with the cyber world, the answer would be surprising, as the spillover of this particular cyber attack has been more than alarming. This is not simply a case of a frozen computer that needs to be fixed. Apart from individual users, the systems of a large number of organizations across the globe were hit by the attack, including critical infrastructure operators, manufacturers and service providers. This means that their systems would stop functioning unless they paid the ransom. The fact that a computer worm managed

[40] Microsoft, 2017.
[41] ENISA, 2017.
[42] Piper, 2017.

to spread all over the world within a few hours with limited resources and cause such a major disruption is unprecedented. Since this is a global-scale cyber attack, it would not be possible to refer separately to every single organization and company affected. However, certain cases that need to be mentioned are Russia – and in particular its interior ministry, railways, banks and mobile phone operators - the UK's National Health Service (NHS), German railways, one of Spain's large telecommunications company, natural gas company and electrical company and many other cases around the world, which among others include a French car manufacturer, Chinese universities, Japanese companies, Indonesian hospitals and the Indian state police.[43] The expansion of the attack was so rapid and so immense that it would not be an overstatement to say that the world experienced a cyber barrage.

The economic losses caused by the attack are indisputably high and are estimated to reach up to US $8 billion.[44] It needs to be highlighted that the losses are not only connected to the ransom itself but the cost was also connected to the disruption of services, vital societal functions and business interruptions, which make the actual impact of the attack far more significant. It is also believed that the cost of the attack could be much higher, if the attackers had chosen more sensitive key targets within critical infrastructure, such as nuclear power plants, or if they had opted for malicious damage instead of financial gains. This should be taken into consideration as it demonstrates the devastating impact such attacks can have and how cyberspace can turn into a hotbed of potential crises.

At this point it is highly significant to make special reference to the attack's impact on the UK's health sector. NHS services across England and Scotland were severely affected by the attack. Hospital and GP appointments were disrupted and certain hospitals and GPs were unable to access patient data. Several ambulances were diverted from hospitals and there were also disruptions in surgeries. Even though there were no reports of harm to patients, the attack affected important medical and diagnostic equipment due to the loss of access to computers.[45] Even in cases where several computers were not affected by the virus, they had to be taken offline in order to reduce the risk of infection. In the official report on lessons learnt after WannaCry, the NHS admits how this attack brought the need for security

[43] For an overview of the countries and organizations severely affected by the attack, see: BBC, 2017b.
[44] According to the risk-modelling company Cyence: Barlyn, 2017.
[45] For more details, see: BBC, 2017a.

improvements to the surface due to the high level of dependence on information technology.[46] The attack's effect on the health sector constitutes a clear illustration of how an attack within the cyber sector can spread to multiple sectors and disrupt services that are vital for the proper functioning of the real world.

How was it handled?

Considering that the WannaCry targeted Microsoft Windows operating systems, it did not come as a surprise that the private sector came to the fore to respond to the attack's unprecedented domino effect. Microsoft immediately released emergency security patches the day that followed the initial attack.[47] This could not reverse the damage that had already been done, but it could at least protect users, and most importantly organizations, from further infections that could be caused by worms similar to WannaCry. At the same time, international organizations together with CERTs and large cybersecurity companies issued guidelines that users should follow in response to the attack, regardless of whether they had been hit or not. Cybersecurity experts advised users against paying the ransom and urged them to update their systems as soon as possible in order to ensure their protection.[48]

However, the impact of the attack could have been far more disruptive had it not been for Marcus Hutchins, a British computer security researcher, also known by the pseudonym "Malware Tech". The researcher accidentally discovered a "kill switch" by registering a domain name that tracked the spread of the virus and in the end halted it.[49] It managed to significantly slow down the worm's spread and allow for the implementation of further measures that would protect against the attack, but it could not repair systems that were already infected. However, this did not mean that the attack was over. The researcher stressed the need for users to update their systems and warned that the world could be hit once again by new variants of the malware that will not be halted by the "kill switch", as there would be no reason for the attackers not to try again since they could have very high profits with limited resources.[50]

Investigations conducted by the FBI, cybersecurity companies, the UK's National Cyber Security Centre and Microsoft itself all concluded that North Korea

[46] Smart, 2018, p. 5.

[47] Microsoft Security Response Center (MSRC) Team, 2017.

[48] Baraniuk, 2017.

[49] For more details on how "Malware Tech" halted the virus from spreading further, see the researcher's blog: Malware Tech, 2017.

[50] Foxx, 2017.

was behind this unprecedented cyber barrage, as they traced the attack to cyber affiliates of the North Korean government.[51] In December of the same year the US publicly announced that it considered North Korea to be the culprit behind the attack, despite the fact that it denied the accusations. Delving deep into the technical details of the investigation or issues regarding attribution would go beyond the scope of the present study and would also touch upon the field of international relations. However, what seems to be of particular interest is the reaction of Brad Smith, the President of Microsoft, in the 14th of May, immediately after the attack and long before the official attribution.

It could be argued that Smith's response scratches the surface of WannaCry and demonstrates the complexity of cyber-related issues. Two days after the initial attack, Microsoft's President initiates a discussion that goes beyond the technical aspects and shows how cybersecurity is a "shared responsibility".[52] Even though it is the company's duty to improve its capabilities and ensure its customers' security, it will never be enough if customers themselves do not share the burden and come to an understanding of how important it is to keep their systems updated. This highlights how vital it is for users to think proactively about the security of their systems and practice good cyber hygiene. The fact that such a large number of computers was still vulnerable, even though Microsoft had released the necessary patches two months prior to the attack, indicates that cybersecurity should not be taken for granted and viewed as the responsibility of a third party.

Moreover, Smith refers to another issue which has proven to be crucial for cybersecurity but due to its sensitivity has not yet been openly discussed: the stockpiling of vulnerabilities by governments. At this point, his argument is worth noting, as it illustrates how governments can bear responsibility for crises in cyberspace, not only by orchestrating a cyber attack but also by leaving the door open to new threats:

> *"[...] this attack provides yet another example of why the stockpiling of vulnerabilities by governments is such a problem. This is an emerging pattern in 2017. We have seen vulnerabilities stored by the CIA show up on WikiLeaks, and now this vulnerability stolen from the NSA has affected customers around the world. Repeatedly, exploits in the hands of*

[51] According to Symantec, the ransomware showed strong links to the Lazarus Group, a group of North Korean-linked hackers: Symantec, 2017a.

[52] Smith, 2017.

> *governments have leaked into the public domain and caused widespread damage. An equivalent scenario with conventional weapons would be the U.S. military having some of its Tomahawk missiles stolen. And this most recent attack represents a completely unintended but disconcerting link between the two most serious forms of cybersecurity threats in the world today – nation-state action and organized criminal action".*[53]

Microsoft's President brilliantly sums up what seems to be a major challenge. Building capacities for offensive purposes in cyberspace is a great risk as it also means that certain vulnerabilities are being stockpiled and kept secret. The danger lies in the fact that a government can never be absolutely certain that these vulnerabilities will not end up in someone else's hands, whether it is another state actor or a cyber criminal.

Initial Observations

All interviewees responded that they consider WannaCry a cyber crisis and a case of transboundary crisis management, as it presents all the criteria required. After examining how the attack unfolded and the initial reactions to it, it is necessary to pinpoint certain characteristics that could add new elements to the concept of the transboundary crisis.

First of all, the speed of the attack's expansion is unprecedented. Even though the rapid escalation of transboundary crises and issues concerning time have been addressed by scholars, it is highly alarming that a threat can expand to the whole world in just a few hours simply by clicking on the wrong buttons. This factor needs to be addressed as it is and will probably continue to be one of the main challenges for the cyber crisis management mechanisms.

Another issue that arises is that of human error and a lack of a general culture of cyber hygiene. The human error plays a very significant role in a potential cyber crisis, as, one minor mistake can have a devastating effect. This does not mean that the human error is not important during a natural disaster for instance. However, in a 'traditional' crisis, there seems to be more space for remediation at least to some extent. In cyberspace, if the mistake is made, there is no turning back, as demonstrated by Wannacry.

[53] Smith, 2017.

Moreover, a crisis in the cyber sector immediately activates crises in multiple sectors. Wannacry demonstrates how one computer worm is enough to cause a crisis that can spread to other domains simultaneously, ranging from political institutions to critical infrastructure. Therefore, a crisis does not initiate from the threat to an IT system since that could be handled with already existing management mechanisms. It initiates from the moment it gets out of control and hits different domains in the real world. As a result, Wannacry demonstrates how cyberspace is used as a tool to simultaneously trigger crises in more than one sectors.

In cyber crises, a primary actor is the private sector. As observed in the case of Wannacry, without Microsoft's mobilization to release patches and handle the situation, the crisis would have escalated even further. This also illustrates Boin's point: traditional crisis management arrangements should be reconsidered,[54] as they run the risk of remaining mere spectators when a modern crisis unfolds and only contribute to the coordination of the actors capable of responding. This also creates an authority vacuum as the crisis' rapid expansion complicates the issue of which actor is responsible for what.[55]

[54] Boin, 2018.

[55] Boin, 2018, p. 2.

Case 2: 2016 Democratic National Committee (DNC) cyber attacks

Attempting to solve the puzzle of cyber crises requires that the researcher examines different cases in order to identify their distinctive features and address certain patterns that emerge. Using cyberspace as a tool to exercise political influence has become an upcoming trend in today's new threat landscape. The case of the US elections might be highly indicative of this trend but it is not the only example. In August 2018, Sweden also experienced slight "cyber turbulence" when the website of the centre-left Social Democrats was hacked twice during the pre-election period and there was a general concern in the country about potential foreign interference with the elections.[56] It is now evident that we are no longer dealing with traditional crises, as, despite the benefits, cyberspace has also allowed potential perpetrators to cause unimaginable damage with very limited resources. It is therefore of utmost importance to take a closer look at the case of the US elections as it could bring to the fore certain characteristics that will enhance our understanding of this new chapter in the crisis debate.

The Chronicle of the Attack: How did it unfold?

The time had come in the US for presidential candidates to prepare for their political battle. 2016's presidential election would later prove to be a turning point in US history but no one could have known that underneath the apparent political debate, a battle was also fought in cyberspace.

Indications of suspicious cyber activity had already shown up since September 2015. The FBI attempted to warn the DNC's IT department that Russian hackers had compromised at least one of their computers but the DNC underestimated the seriousness of the situation and the tech-support contractor who was responsible for investigating the issue did not find anything that could cause concern.[57] A similar attempt took place in November of the same year but the IT department failed once again to address the severity of FBI's warnings. However, the subsequent course of events would reveal how ignoring the signs would be detrimental to the integrity of the US political institutions, as the DNC's network was infiltrated long before the hackers made their presence felt.

[56] Jakobson, 2018.

[57] For an interesting analysis of how the severity of the situation was underestimated, see: Lipton, Sanger and Shane, 2016.

The DNC became aware of the threat in an unexpected way and only when it was already too late. In March 2016, John Podesta, who was at the time chairman of Clinton's presidential campaign, received a seemingly innocent email, masked as an alert from Google, which asked him to immediately change his password by clicking on a link to a page, as his account was supposedly compromised. The chairman could not imagine that this email would, among other reasons, lead to the Democrats losing the 2016 presidential election. At first, Podesta did not change the password, but instead he turned to his assistant who would then consult someone from the DNC's IT help desk. And that was the moment that would later prove detrimental for Clinton's campaign. The IT person responded to Podesta's assistant with a typographical error and, instead of typing "illegitimate", he wrote that the email was "legitimate", which thus led to Podesta clicking on the link. This simple error was enough to activate the spear-phishing email and allow Russian hackers to obtain unhindered access to sensitive information.[58]

The next two months was a period of increasing confusion as to who was behind the attack and gained access to the DNC's computer system. While it was still not officially announced by the investigators that the hackers were directed by the Russian government, CrowdStrike, a cybersecurity company working for the DNC, published its findings and identified two separate hacking groups affiliated with Russian intelligence, "Cozy Bear" and "Fancy Bear".[59] At the same time, another hacker under the pseudonym "Guccifer 2.0" showed up to claim responsibility for the DNC hack in an attempt to cover up Russia's interference, while Donald Trump offered his own explanation asserting that the DNC hacked itself as a way of redirecting public opinion.[60] This shows how, even before any information was leaked, the attack itself caused such a major political turbulence.

The situation took a turn for the worse when in July 2016, a few days before the Democratic National Convention, WikiLeaks published almost 20.000 emails which were in the website's possession after the DNC hack. The emails revealed that the DNC undermined Bernie Sanders and favored Hillary Clinton instead of being impartial,[61] and resulted in the resignation of several senior DNC officials.[62] In

[58] For an interesting article on the course of events and an interview of John Podesta on the issue, see: Sciutto, 2017.
[59] For the official announcement on the company's website, see: Alperovitch, 2016.
[60] Bradner, 2016.
[61] For more details on the content of the emails, see: Schleifer and Scott, 2016.

August, personal cell phone numbers and private email addresses of the Democratic Congressional Campaign Committee (DCCC) were also published, thus leading the US to what the House Minority Leader Nancy Pelosi described as an "electronic Watergate".[63] The FBI officially initiated the investigation but, at least at first, refrained from linking the cyber attacks to any particular actor.[64] However, it was more than obvious that Russia was considered a major suspect, even though President Putin remained firm on his stance that the Russian government had no involvement in the attack or ties to the hackers.[65] During this period of major political turmoil, with presidential candidates crossing swords in the midst of a hacking frenzy, WikiLeaks kept releasing more and more emails, which reached the number of 58.000, even two days before the election.[66]

The result is already known and a source of major political concern not only within the US but globally. It is not a coincidence that the issue is in the media spotlight until today and will probably continue to trigger discussions on the people's democratic rights being called into question. Even though voting machines or computers were not breached, it is without doubt alarming that a battle fought out of public view, in a digital domain that seems hard to grasp, can have such a significant effect on democracy and the people's right to elect their leader. One could not help but wonder: what if the DNC was not hacked? Would Donald Trump still be the President of the US? Was the information leaked significant enough to influence people's choice? How is it possible for a third actor to interfere with people's democratic rights and, by attacking with "ones and zeros", change the course of history?

How was it handled?

As indicated by the investigations that followed the attack, a highly aggravating factor was not the hacking per se, but the way it was handled. The response of the officials responsible for dealing with the issue illustrates that they did not have a clear understanding of the severity of the situation – which seems to be one of the most common problems in cyberspace – and therefore underestimated the threat.

[62] Lopez and Becker, 2016.

[63] Kopan, 2016.

[64] The situation changed when in, 2017, the US Intelligence Community officially reported Russian interference in the DNC hack and the US elections: CIA, FBI and NSA, 2017.

[65] For an interview of Vladimir Putin on the issue, see: Rudnitsky, Micklethwait and Riley, 2016.

[66] Eder, 2016.

Both the FBI, which was supposed to inform the DNC about the breach, and the DNC officials, who were in charge of making the necessary decisions to respond to the attack, made a series of mistakes which would later prove crucial for the course of events. On the one hand, the FBI was accused of a rather "laid-back approach" with unclear warnings.[67] When it became aware of the breach in September 2015, the agency chose to inform the DNC simply by making a phone call. In particular, an FBI agent contacted the DNC's IT department and informed the tech-support contractor, who was on duty at the time, that the DNC's network had been breached by a hacker group called "the Dukes". Since the FBI chose not to raise the alarm and send an official delegation to the DNC, it did not come as a surprise that the DNC's tech-support contractor doubted the validity of their claims and even suspected that it could have just been a prank call. If the FBI had addressed the issue in a more appropriate manner, it would have helped the DNC realize faster that the situation was critical and that response measures should have been taken much earlier.

On the other hand, it was the duty of the Committee's IT department to examine the validity of the FBI's warnings more thoroughly and pass the message on to senior officials. Bearing in mind that those working within this field are more aware of the nature of cyber threats, they should thus be more suspicious and consider every eventuality. Instead, the tech-support contractor did what an average person would do; search on Google. He googled the Dukes but found nothing that could support the FBI's claims. As a consequence, he did not inform his superiors about the FBI's warnings, especially since he did not trace any suspicious activity or signs of a breach in the system. This rather naïve response to the situation resulted in the hackers going unnoticed and having unhindered access into the Committee's network and all its sensitive information for months, until the DNC hired consultants from private cyber security firms.[68] It cannot be stated with great certainty that if the DNC officials were aware of the severity of the situation, none of this would have happened. However, the number of the emails leaked could have been much smaller and sensitive information might not have been exposed to public view.

[67] Harding, 2016.

[68] Hosenball, Walcott and Menn, 2016.

Initial Observations

The DNC hacking case is illustrative of how a phishing email accompanied with a series of communication failures can lead to a major cyberattack targeting at the core of the people's democratic rights.

At this point, it should be mentioned that the interviewees did not have a firm response as to whether or not the DNC hacking during the US elections constitutes a cyber crisis or not, as, even though there is an obviously devastating political impact, this case lacks a major IT disruption or disruption of services, as for instance in the case of WannaCry. However, when asked about the nature of a cyber crisis, all interviewees highlighted the fact that one of the most significant characteristics of a cyber crisis is the paradigm shift from causes to impacts. If an IT disruption is successfully managed and has no actual societal impact, it does not constitute a crisis, regardless of how severe it might be at a technical level. On the contrary, if a very small disruption has a direct societal impact or poses a threat to the values of a system, it can fall within the crisis category, even if it is not a major IT disruption. And this is also the reason why we refer to cyber crises and not IT crises, as the term cyber incorporates more aspects and domains that interact with each other.

Another distinctive characteristic this case illustrates is how a cyber attack can cause both an institutional crisis and a crisis of trust, a factor that was also pointed out by the interviewees. How can the public be reassured that there have been no more breaches and the attacks have been terminated when even democracy itself is being questioned? How can the people continue to trust public institutions after the structural deficiencies revealed by the attack? Since cyberspace allows for threat agent masquerading, how can the public be certain about the attack's culprits? Is it Russia, guccifer or maybe someone else?

Summary of the Findings

After some initial observations on the attacks and the way they unfolded, combined with the cybersecurity experts' input, the following chapter summarizes the main findings of the cases' examination, most of which apply to both cases, and makes it easier for the reader to keep track of potential challenges during a cyber crisis:

1. Significant difficulty in detecting the breach and making sense of the threat, which usually results in slow responses.

2. Unprecedented speed of the threat's expansion, which makes it difficult for decision makers and academics to identify when the crisis starts and when it ends.

3. The factor of human error plays a much more significant role during a cyber crisis, as demonstrated by both of the cases.

5. A crisis in the cyber domain immediately activates a crisis in another domain or in multiple domains (this could also be the case in conventional crises, but here cyberspace is actually used as the means by which damage is caused to multiple sectors).

6. One vulnerability is enough for an attack to spread to hundreds of thousands of users.

7. Great challenges regarding who is responsible for handling each phase of the crisis (authority vacuum).

8. Threat agent masquerading, which causes major difficulty in terms of attribution.

9. Need to manage both the disruption to the IT system itself (technical aspect) and the "physical" or traditional crisis.

10. Every cyber attack is always the result of human activity, which means that, in contrast to e.g. a natural disaster, there is always someone, either a state actor or an individual, that controls the attack and subsequently controls, at least to some extent, the course of events.

11. Determining the victim is another challenge area in cyber crises. Even though the targeted organization will always be the victim, at the same time, the lack of proper cybersecurity measures automatically turns the organization into a culprit.

17. Need for cooperation and coordination among people from very different sectors and areas of expertise in a timely manner and under conditions of urgency and uncertainty.

19. Dilemma as to whether or not the management of the cyber crisis should be the responsibility of a centralized hub or of crisis management mechanisms distributed within different sectors.

20. Paradigm shift from the causes of the crisis to its impact.

Conclusion

One thing is certain: the world of crises has changed and is still changing. Failing to address the issue and avoiding to delve deeper into issues that might at first seem difficult to grasp will result in either overreacting or underreacting to potential threats. It is the role of academics to identify these changes and push for institutional adaptation.

After examining certain cyber cases and studying their distinctive features, it is argued that the root of the puzzle and the terminological haziness is the use of traditional concepts to explain new threats. Policy makers and academics do not need to expect “cyber doom scenarios” with “technology out of control” in order to start talking about a cyber crisis.[69] The present paper demonstrates how both of these cases should be characterized as cyber crises. It argues that the reason why they were not characterized as such was because of an academic reluctance to touch upon the issue and also because of a “one size fits all” logic, with cyber crisis experts borrowing terms from traditional crisis management.

The digital world has been largely overlooked by crisis academics. It is true that the impact of a potential cyber crisis does not manifest itself in the same way as for instance a natural disaster. However, the fact that we have not come to a better understanding of the new threat landscape and the new nature of crises and hesitate to take part in the crisis debate does not mean that the crisis is not there. Following the academic turmoil in the field of security studies, with researchers moving from a more realist perspective to the direction of broadening the agenda to include new

[69] For an analysis on the plausibility of “cyber doom scenarios” see: Lawson, 2013.

dimensions such as the individual and the society, the crisis management field also needs to bring new perspectives to the table and keep up with the shifting nature of crises. In today's technologically interconnected world, this could not be accomplished without studying the distinctive features of cyberspace and what they can add to the academic discussion.

These particular case studies demonstrated how dangerous a cyber crisis can be and how quickly it can escalate into something no one could predict. And this is the case today. Tomorrow, with the rapid development of the Internet of Things and the rise in the level of interconnectedness, a potential cyber crisis could be devastating, unless we establish a proactive stance on the matter. Drawing from Rhinard, who describes transboundary management capacity as a collective good,[70] it is indeed time to realize that the shift towards a new crisis concept requires that we view its management as a shared responsibility.

Venues of Future Research

The present paper argues that by using traditional crisis concepts to explain new threats, we fail to establish certain cyber attacks as cases of transboundary crises. Apart from the obvious choice of delving into more cases of cyber attacks to test the theory, an excellent venue of future research could be the examination of already existing crisis management models and how effective they are in the new threat landscape. Traditionally, crisis management models are more "process-oriented", as they follow the traditional time sequence of events. Are these models still applicable to the new transboundary crises or should we move towards a "scenario-driven" approach, with multiple scenarios for multiple sectors? How does the cyber sector and potential cyber attacks affect the already existing models?

Another interesting research proposal, which is actually one of the present study's limitations, is to examine the effectiveness of cyber crisis management mechanisms in response to major cyber attacks that could fall within the crisis category. Can these mechanisms effectively respond to such threats or should we reconsider our crisis management arrangements? Which type of crisis management would work better in a cyber crisis? A centralized cyber crisis management capacity

[70] Rhinard, 2009.

with a central hub responsible for coordinating all other actors, or a distributed cyber crisis management with different layers of jurisdiction among different sectors?

Finally, for researchers also interested in international relations while still remaining within the crisis concept, it would be interesting to look into different cases and examine where we could draw a line between cyber crises and cyber warfare. Which are the factors that determine whether a case falls within the former or the latter category and how can an answer to this question contribute to a better understanding of the two concepts?

References

Books, Articles and Papers

Alvesson, M. and Sandberg, J. (2011). Generating research questions through problematization. *Academy of Management Review, 36*(2), pp. 247-271.

Ansell, C., Boin, A., and Keller, A. (2010). Managing transboundary crises: Identifying the building blocks of an effective response system. *Journal of Contingencies and Crisis Management*, 18(4), pp. 195–207.

Ansell, C., Boin, A. and Kuipers S. (2016). Institutional Crisis and the Policy Agenda. In N. Zahariadis, (Ed.), *Handbook of Public Policy Agenda Setting.* Cheltenham, UK: Edward Elgar Publishing Ltd. pp. 415-432.

Backman, S. (2016). *The Institutionalization of Cybersecurity Management at the EU-level 2013-2016*. Stockholm: Swedish Defence University.

Bergström, G. and Boréus, K. (2017). *Analyzing Text and Discourse.* London: Sage.

Boin, A. (2004). Lessons from Crisis Research. In B. W. Dayton (Ed.), Managing Crises in the Twenty-First Century. *International Studies Review*, 6(1), pp. 165-194.

Boin, A. (2005). Disaster Research and Future Crises: Broadening the Research Agenda. *International Journal of Mass Emergencies and Disasters*, 23(3), pp. 199-214.

Boin, A. (2009). The New World of Crises and Crisis Management: Implications for Policymaking and Research. *Review of Policy Research*, 26(4), pp. 367-377.

Boin, A. (2018). The Transboundary Crisis: Why we are unprepared and the road ahead. *J Contingencies and Crisis Management*, pp. 1-6.

Boin, A., Ekengren, M., and Rhinard, M. (2014). Transboundary crisis governance. In J. Sperling (Ed.), *Handbook of Governance and Security*. Cheltenham, UK: Edward Elgar Publishing Ltd. pp. 307-323.

Boin, A., ‘t Hart, P. (2000). Institutional Crises and Reforms in Policy Sectors. In: H. Wagenaar (ed.), *Government Institutions: Effects, Changes and Normative Foundations*. Library of Public Policy and Public Administration, vol 5. Dordrecht: Springer. pp. 9-31.

Boin, A., ´t Hart, P., Stern, E., and Sundelius, B. (2005). *The Politics of Crisis Management: Public Leadership under Pressure*. Cambridge: Cambridge University Press.

George, A., L. and Bennett, A. (2005). *Case Studies and Theory Development in the Social Sciences.* The Belfer Center for Science and International Affairs, MIT Press.

Gustafsson, K. and Hagström, L. (2017). What Is the Point? Teaching Graduate Students how to Construct Political Science Research Puzzles. *European Political Science,* pp. 1-15.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security,* 2(4), pp. 49-60.

Lagadec, P. (2009). A New Cosmology of Risks and Crises: Time for a Radical Shift in Paradigm and Practice. *Review of Policy Research,* 26(4), pp. 473-486.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics,* 10(1), pp. 86-103.

Perrow, C. (1999). *Normal Accidents: Living with High Risk Technologies*. Princeton, NJ: Princeton University Press.

Rhinard, M. (2009). European Cooperation on Future Crises: Toward a Public Good?. *Review of Policy Research,* 26(4), pp. 439-455.

Rosenthal, U., Charles, T., M. and Hart, t’ P. (1989). The World of Crises and Crisis Management. In U. Rosenthal, M. T. Charles, and P. 't Hart (Eds.), *Coping with Crises: The Management of Disasters, Riots, and Terrorism*, Springfield, IL: Charles C.

Rosenthal, U. and Pijnenburg, B. (1991). Simulation-oriented scenarios: an alternative approach to crisis decision making and emergency management. In U. Rosenthal and B. Pijnenburg (eds.), *Crisis Management and Decision Making: Simulation Oriented Scenarios*, pp. 1-7. Dordrecht: Kluwer Academic Publishers.

Shapiro, I. (2002). Problems, methods, and theories in the study of politics, or what's wrong with political science and what to do about it. (Section II: Political theory, political science, and politics). *Political Theory, 30*(4), pp. 596-619.

Steinar, K. (1996). *InterViews: An Introduction to Qualitative Research Interviewing*. London: Sage.

Official Reports

CIA, FBI and NSA. (2017). Assessing Russian Activities and Intentions in Recent US Elections. *Intelligence Community Assessment*. Retrieved from https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Smart, W. (2018). *Lessons learned review of the WannaCry Ransomware Cyber Attack*. Independent Report. London: Department of Health & Social Care.

Trimintzios, P., Holfeldt, R., Koraeus, M., Uckan, B., Gavrila, R. and Makrodimitris, G. (2014). Report on Cyber Crisis Cooperation and Management: Comparative study on the cyber crisis management and the general crisis management. *ENISA*. Retrieved from https://www.enisa.europa.eu/publications/ccc-study.

Online Sources

Alperovitch, D. (2016, June 15). Bears in the Midst: Intrusion into the Democratic National Committee. *CrowdStrike*. Retrieved from https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

Baraniuk, C. (2017, May 15). Should you pay the WannaCry ransom?. *BBC News*. Retrieved from https://www.bbc.com/news/technology-39920269.

Barlyn, S. (2017, July 17). Global cyber attack could spur $53 billion in losses: Lloyd's of London. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB.

BBC. (2017a, May 13). *NHS cyber-attack: GPs and hospitals hit by ransomware*. Retrieved from https://www.bbc.com/news/health-39899646.

BBC. (2017b, May 15). *Ransomware cyber-attack: Who has been hardest hit?*. Retrieved from https://www.bbc.com/news/world-39919249.

Bradner, E. (2016, June 16). Trump: DNC hacked itself. *CNN*. Retrieved from https://edition.cnn.com/2016/06/15/politics/dnc-hack-donald-trump/.

Eder, S. (2016, November 8). Julian Assange Releases More Emails and Defends WikiLeaks' Mission. *The New York Times*. Retrieved from https://www.nytimes.com/2016/11/09/us/politics/julian-assange-wikileaks-emails.html.

ENISA. (2017, May 15). *WannaCry Ransomware Outburst*. Retrieved from https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst.

Europol. (n.d.). *Wannacry Ransomware*. Retrieved from https://www.europol.europa.eu/wannacry-ransomware.

Foxx, C. (2017, May 13). Global cyber-attack: Security blogger halts ransomware 'by accident'. *BBC News*. Retrieved from https://www.bbc.com/news/technology-39907049.

Guion, P. (2015, February 13). US President Obama says cyber-security among greatest challenges. *The Independent*. Retrieved from https://www.independent.co.uk/news/world/americas/us-president-obama-says-cyber-security-among-greatest-challenges-10045950.html.

Harding, L. (2016, December 14). Top Democrat's emails hacked by Russia after aide made typo, investigation finds. *The Guardian*. Retrieved from https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds.

Hosenball, M., Walcott, J. and Menn, J. (2016, August 3). FBI took months to warn Democrats of suspected Russian role in hack: sources. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-cyber-democrats-reconstruct/fbi-took-months-to-warn-democrats-of-suspected-russian-role-in-hack-sources-idUSKCN10E09H.

Jakobson, H. (2018, August 10). Attacker slog ut Socialdemokraternas hemsida. *Dagens Nyheter*. Retrieved from https://www.dn.se/nyheter/politik/riktad-attack-mot-socialdemokraternas-hemsida-/.

Kopan, T. (2016, August 11). Nancy Pelosi: DNC hack is 'electronic Watergate'. *CNN*. Retrieved from https://edition.cnn.com/2016/08/11/politics/dnc-hack-electronic-watergate/.

Lipton, E., Sanger, D. E. and Shane, S. (2016, December 13). The Perfect Weapon: How Russian Cyberpower Invaded the U.S. *The New York Times*. Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Lopez, L. and Becker, A. (2016, August 2). Senior Democratic National Committee officials resign: DNC. *Reuters*. Retrieved from: https://www.reuters.com/article/us-usa-cyber-democrats/senior-democratic-national-committee-officials-resign-dnc-idUSKCN10D209.

Malware Tech. (2017, May 13). *How to Accidentally Stop a Global Cyber Attacks*. Retrieved from https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.

Microsoft. (2017, March 14). *Microsoft Security Bulletin MS17-010 – Critical*. Retrieved from https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010.

Microsoft Security Response Center (MSRC) Team. (2017, May 12). Customer Guidance for WannaCrypt attacks. *Microsoft TechNet*. Retrieved from https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/.

Nakashima, E. and Timberg, C. (2017, May 16). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html?utm_term=.f3dca304670a.

Passeri, P. (2018, October 11). September 2018 Cyber Attacks Statistics. *Hackmageddon*. Retrieved from https://www.hackmageddon.com/2018/10/11/september-2018-cyber-attacks-statistics/.

Piper, E. (2017, May 14). Cyber attack hits 200,000 in at least 150 countries: Europol. *Reuters*. Retrieved from https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX.

Rudnitsky, J., Micklethwait, J. and Riley, M. (2016, September 2). Putin Says DNC Hack Was a Public Service, Russia Didn’t Do It. *Bloomberg*. Retrieved from: https://www.bloomberg.com/news/articles/2016-09-02/putin-says-dnc-hack-was-a-public-good-but-russia-didn-t-do-it.

Schleifer, T. and Scott, E. (2016, July 25). What was in the DNC email leak?. *CNN*. Retrieved from https://edition.cnn.com/2016/07/24/politics/dnc-email-leak-wikileaks/.

Sciutto, J. (2017, June 28). How one typo helped let Russian hackers in. *CNN*. Retrieved from https://edition.cnn.com/2017/06/27/politics/russia-dnc-hacking-csr/index.html.

Smith, B. (2017, May 14). The need for urgent collective action to keep people safe online: Lessons from last week’s cyberattack. *Microsoft*. Retrieved from https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

Symantec. (2017a, May 22). *WannaCry: Ransomware attacks show strong links to Lazarus group*. Retrieved from https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group.

Symantec. (2017b, October 23). *What you need to know about the WannaCry Ransomware*. Retrieved from https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack.