Vrije Universiteit Amsterdam

Universiteit van Amsterdam

Master Thesis

From Commons to Exclusion Patterns of Securitization

Author: Will Bergen (2539950)

1st supervisor: Professor Gerard Alberts
2nd reader: Professor Herbert Bos

A thesis submitted in fulfillment of the requirements for the joint UvA-VU Master of Science degree in Computer Science

July 12, 2019

"I am the master of my fate, I am the captain of my soul"
from Invictus*, by William Ernest Henley*

Abstract

The pattern of securitization is common, in events ranging from terrorist incidents like the attack on 9/11 to the Russian meddling in the US election of 2016. Within each, a notion of security emerged which was unique with regard to the space, and to the traditions there-enshrined. Further, in such cases, there appears a pattern of emerging tragedy and resultant exclusion, which collectively securitizes the organization, structures or space. The history of computing security contains many such events, and considering them historically provides a lens through which to better understand the nature of securitization and suggest larger patterns. In doing so, the dynamic nature of securitization emerges through its apparent dependence on the forms that tragedy and exclusion take. This analysis is aided by explicitly considering several common computer security concepts, as well as the tragedy of the commons, and various forms of exclusion. Using these tools, we consider how the interaction of pre-digital forms with digital technology may affect the pattern of securitization. In particular, we trace the power of tradition on forms of exclusion as digital technology creates increasingly diverse new spaces, and distributes them across increasingly disparate zones of authority.

From Commons to Exclusion

Contents

1

Introduction

When two passenger jets crashed into the World Trade Center towers in New York City on September 11th, 2001, the way we think about commercial airlines was fundamentally changed. No longer were they simply modes of transport; they became weapons. The airline industry, and the broader issue of international terrorism were thus securitized. An entirely new security agency emerged, aggressive new security measures were introduced at airports, security personnel were embedded on many flights, and a war was launched. In practice, American airports developed a new, oppressive feeling dominated by stern instruction and increasingly invasive screening procedures: all in the name of security. This phenomenon, what we here term securitization, in the context of 9/11 would seem to consist of a tragedy, and a response.

Abstractly, this pattern of threat identification and reaction, what one might term 'security emergent', is common. Something, be it an act of violence, a critical mass of fear, or the discovery of a new mode of interaction leads to security-oriented rhetoric and securitizing action. As someone who can recall exactly where he was during the 9/11 attacks, and as a citizen of a country which has for nearly two decades now been dominated by the fallout from those attacks, this phenomenon is particularly poignant. What appears particularly interesting are potential parallels between the physical domain, with its long history of such events, and the digital domain, which is still in its infancy. Despite the relative youth of the computers and cyberspace, the digital domain is in no way lesser than its older siblings.

The capacity for digital disruption and violence has been demonstrated many times over, in a dizzying array of forms ranging from Stuxnet's retardation of the Iranian nuclear program to the dissemination of the Columbine shooters' journals[1], and from nationwide

1. Peter Langman, "Role models, contagions, and copycats: An exploration of the influence of prior

cyber attacks like those launched against the Ukraine, Georgia and Estonia over the past decade to the 2016 US election meddling and global malware-based schemes like Gameover Zeus and Wannacry. Further, digital technologies have become a core component of the US military's doctrine; especially since their demonstratively successful use in the 1991 operation Desert Storm, after which other nations - most particularly China[2] - began to implement similar, technology-driven, continuous revolutions in their military affairs.[3] Desert Storm also saw a group of Iraqi soldiers surrender to an unmanned aerial vehicle in the first known event of its kind.[4] Clearly, the digital domain, both in its own right and as it supplements other theaters is as real, serious, and potentially lethal as any other.

Given these parallels there are clear benefits to better understanding how phenomena clearly present in the non-digital domains, like that of securitization, behave digitally. For this reason, we have undertaken to explore this notion through a variety of case studies: digital-age events during which notions of security emerged. From the outset of the work, there have appeared several abstract conceptualizations which seem to be omnipresent, and which, if explored, may provide insight into the inherently digital nature of modern securitization. These concepts include the 'Tragedy of the Commons', and exclusion.

The Tragedy of the Commons refers to the way in which a shared good's use-value is degraded over time. In the absence of generally respected rules on its use, the good is damaged and eventually rendered largely useless as individuals make additional demands upon it, naively intuiting that - in the short term - the benefits will accrue directly to them, while the good's entire user base will share the costs. A further abstraction has also seemed valuable with regard to the case studies we have investigated: that of a loss of innocence. It is not difficult to see the aforementioned naivety as innocence: innocence necessarily lost when the resource's degradation reaches a critical point. This loss of innocence formulation provides a salient within which to capture 9/11 under the umbrella of the tragedy of the commons. Though the vast majority of pre-9/11 air travelers were not making anti-social demands upon the system, our collectively updated understanding of the damage one ill-intentioned flyer could cause prompted us into a state which necessarily assumed anyone could be such a bad actor. A critical point had been reached.

killers on subsequent attacks," *Available on www. schoolshooters. info*, 2017,

2. Andrew Scobell, David Lai, and Roy Kamphausen, *Chinese Lessons from Other Peoples' Wars*, technical report (ARMY WAR COLL STRATEGIC STUDIES INST CARLISLE BARRACKS PA, 2011).

3. This idea is usually referred to as Revolution in Military Affairs, or RMA; Joseph Henrotin, *The Art of War in the Network Age: back to the future*, vol. 1 (Wiley Online Library, 2016).

4. Peter W Singer, "Military robots and the laws of war," *The New Atlantis*, no. 23 (2009): 25–45.

In response to a commons or commons-like resource reaching that critical point, the common's security is considered, and assuming it is deemed valuable, some mechanism for its protection is implemented. Broadly speaking, this mechanism usually takes the form of some exclusionary act. For instance, in the case of an individual making demands of a common above and beyond her sustainable share, she might be excluded from its use. From the earliest days of the digital age, literal forms of exclusion have formed a core component of security, from locking the doors of computing centers, to the now ubiquitous use of passwords. Post-9/11 security measures included literal means of exclusion designed to keep would-be attackers physically away from airplanes, as well as the assignation of the status of 'other' to a very particular group of people. The constant presence of exclusion in such a variety of forms is core to why it is an interesting concept to look at with respect to securitization, and our events are chosen in part to canvas this spectrum.

Through exploring these case studies, and considering them in terms of both the Tragedy of the Commons and exclusion, as well as in terms of modern cyber security - particularly notions like that of a threat-model and an attack surface - we hope to improve our grasp of digital securitization, both as it parallels non-digital domains, and takes on its own unique qualities. To facilitate this investigation, we have chosen a series of events with a mind toward their diversity. Through events varied with regards to technologies, actors and traditions, we hope to gain a better sense of the securitization paradigm we are interested in. The cases, and the reasons they have been selected are as follows.

The first case we will consider, in chapter 4, is the 1970 passage of the Fair Credit Reporting Act (FCRA) which implemented federally-empowered exclusion of bad credit-reporting practices at the behest of the public. This event provides a tailor-made entry point to our exploration for two reasons. The first is that legislation in response to public outcry is a time-honored tradition, with the roles of crier and enforcer well defined. In comparison with the new spaces and loosely or undefined roles which have appeared in just the last several decades of the digital age, the FCRA is representative of a powerful, traditional paradigm featuring common tragedy and resultant exclusion. Second, the 1960s, during which the outcry reached its peak, was a time when the public was just starting to become aware of computerization, and react negatively toward what was beginning to be perceived as its potential to dehumanize. The event therefore establishes a beginning for our exploration of computer-era securitization at the boundary of the pre-digital and digital ages. We will also take advantage of this event to fully operationalize the tragedy of the commons in terms of our work.

In chapter 5, we will consider the story of, and securitization represented by, Robert Morris' release of his now infamous worm in 1988. The event combined headlines with real dollar costs in a way that the computing world had not seen before. Though computer-insider evangelists and public media had for over a decade been speaking to the dangers of lax computer security, Morris' worm, released just prior to the dawn of the Web, in many ways represented a watershed combination of qualities. Of particular interest here, are the assumptions upon which the then-Internet functioned that Morris' worm disrupted. For instance, while Morris certainly fit the digital-miscreant profile popular at the time, the damage he caused massively exceeded expectations.

Next, in chapter 6, we will investigate the story of the Dutch computing center at the Centrum Wiskunde & Informatica (CWI) in Amsterdam. With the aid of first hand accounts of the evolution of a computing center as PCs and networks became the dominant model of computer use, we will investigate the traditions and culture of the CWI's Computer Systems and Telematics (CST). Based in this culture, the CWI provides a lens through which to consider how, as modes of access to computing resources transitioned from personal and physical to anonymous and distributed, security precepts changed with it.

In chapter 7, we zoom in on an example of an early Internet-enabled commons, and the emergent difficulties in securitizing a space for which no tradition existed, save that of the space's architects. With the help of Michael van Eeden, we look at Amsterdam's Digital City initiative of the early 1990s, and the pre-web, personal space called the *Metro* that Mr. van Eeden built within it. Faced with unexpected community-damaging behavior within his system, Mr. van Eeden was forced to make decisions which at first glance appear highly antithetical to his well-credentialed hacker background. Our proximity to the event gained through Mr. van Eeden provides an opportunity to examine securitization in microcosm, and, similar to the FCRA, through the lens of an event concurrent with the advent of groundbreaking technology and what has today become so ubiquitous as to often be misconstrued as the Internet itself: the World Wide Web. The relatively micro nature of the Metro also provides an entry point for considering how the increasing ease and speed with which new modes of interaction are developed today may affect securitization. That same micro nature also provides relatively clear-cut examples of each of our component themes.

Having zoomed in on the Metro, we next zoom out to consider the 2007 cyber attacks on Estonia in chapter 8. By couching the event's narrative in the history of antagonism between Russia and Estonia, we attempt to trace the paradigms of tragedy and exclusion

into the modern cyber landscape, complete with nation-state actors and an ever increasing ubiquity of digitization, from governance to warfare. Like the Metro in the early 1990s, in 2007, antagonistic cyber interaction between nation-states lacked historical precedent. However unlike the Metro, where there was at least a fairly obvious authority to turn to in the form of Mr. van Eeden, Estonia could not so easily exclude behavior it did not like through appealing to a greater, external power. Despite this, Estonia managed to functionally improve their exclusion of Russian activity. Their response provides important insight into patterns of exclusion as it exists when there is no higher authority to turn to.

Finally, in chapter 9, we investigate the recent Russian meddling in the 2016 US presidential election. Drawing heavily on the recently released Mueller report, we are able to couch our analysis in a concrete, well-evidenced story of Russian social engineering and information warfare played out over the last three years. Having entered the current age through the FCRA, the most recent major development in cyber conflict seems an apt finale. Further, while the meddling and its aftermath clearly represent securitization, and to a large extent follow the Estonian model of exclusion without an immediately available authority, the sheer effectiveness of the Russian disinformation campaign gives one pause. While Estonia, for a variety of reasons, chose not to take retaliatory action against Russia, the US has very recently begun to flex its own cyber capabilities, precipitating a generally more hostile, heavily securitized global cyber landscape. The story of recent election meddling and related hacking powerfully attests not only to the danger from a widespread, tragedy-inducing lack of moral-restraint, but to the difficulty of cyber total war.

It remains to relativize our use of the term securitization in the context of our work here. *Securitize* has come to, most popularly, refer to the financial act of "converting illiquid assets into liquid securities."[5] *Securitization* then is "a financing technique by which homogeneous income-generating assets − which on their own may be difficult to trade − are pooled and sold to a specially created third party, which uses them as collateral to issue securities and sell them in financial markets."[6] This financial securitization is widely considered to have contributed to the 2008 financial crisis by, inter alia, increasing the system's reliance on external risk assessors and complicated modeling.[7]

Another common use of the term *securitization* in academia and political spheres comes from the Securitisation Theory of the so-called Copenhagen School of international re-

5. Benjamin J Keys et al., "Did securitization lead to lax screening? Evidence from subprime loans," *The Quarterly journal of economics* 125, no. 1 (2010): 307–362.

6. Angelos Delivorias, "Understanding Securitisation: Background, Benefits, Risks," *European Parliament Research Service, PE569* 17 (2016).

7. Ibid.

lations.[8] This use is much more interesting from our perspective, and has to do with the dialectic interaction between declaring something to be a "security" issue, and the potential force which a polity or other authority may exert *over* the issue, or exert generally *because* of the issue. In their foundational 1998 work *Security: A New Framework for Analysis*, Barry Buzan, Ole Wæver and Jaap de Wilde describe securitization as an extreme form of politicization:

"'Security' is the move that takes politics beyond the established rules of the game and frames the issue either as a special kind of politics or as above politics. Securitization can thus be seen as a more extreme version of politicization."[9]

Elaborating, they describe securitization in terms of a state's interaction with an issue. As opposed to a non-politicized issue which the state doesn't deal with at all, a securitized issue is one presented by the state as an "existential threat". In doing so, the state "justif[ies] actions outside the normal bounds of political procedure."[10] Finally, Buzan et al. describe successful securitization as having three components: "existential threats, emergency action, and effects on interunit relations by breaking free of rules."[11] This enumeration of their securitization well-captures 9/11: from the development of the existential threat of international terrorism, to the enactment of security measures clearly above and beyond traditionally allowed state roles (i.e. the NSA's interpretation of section 215 of the Patriot Act[12]). This operationalization of securitization parallels our use of the term in this work, with several important differences.

First, Buzan et al.'s definition implies agency on the part of the state which clearly seeks greater power in the face of existential threats. we are uninterested in attempting to value any quality of outcome, and rather focus on understanding how variation in contributing forces affects the character of the response to perceived tragedy - what in Buzan et al.'s terms would be the "emergency action." Second, and more generally, we are interested specifically in the first two components: our definition of securitization excludes their last step. We focus here on the emergence of threats, existential or otherwise, and the nature of the reaction. Finally, our work is specific to the fields of computing and those areas and spaces enabled or directly affected by computing technologies.

8. Claire Wilkinson, "The Copenhagen School on tour in Kyrgyzstan: Is securitization theory useable outside Europe?," *Security dialogue* 38, no. 1 (2007): 5–25.

9. Barry Buzan et al., *Security: A new framework for analysis* (Lynne Rienner Publishers, 1998).

10. Ibid., 24.

11. Ibid., 26.

12. Susan Landau, "Making sense from Snowden: What's significant in the NSA surveillance revelations," *IEEE Security & Privacy* 11, no. 4 (2013): 54–63.

...

2

Status Quaestionis

2.1 Humans, Diversity and Holism

Recently, the Computer Security field has begun attempts to come to terms with its growing diversity. Speaking at Black Hat USA 2018, Parisa Tabriz, heading the team in charge of the security of Google's Chrome browser, called for a culture of defense.[13] At the same event, Black Hat's founder Jeff Moss spoke to the presence of clashing models of security between the business and political worlds.[14] In a recent SANS Institute presentation *The Five Most Dangerous New Attack Techniques*, the need for cyber security training was emphasized[15], in keeping with similar calls as made, for instance, by Steven Furnell.[16] In a statement that manages to at once convey the goals of the field, and underline the distance yet to cover, Furnell opens his editorial by saying "Human aspects are now widely recognized as being a key factor in providing a holistic cyber security solution." While it is now more common for authors to take such a holistic tack in Computer Science literature on security, and while human factors are now being considered more often, upon reflection the suggestion that this is a new realization seems odd.

In 1970, *Security Controls For Computer Systems*, commonly known as the *Ware Report*, was published by the Defense Science Board - an advisory panel to the US Department of Defense (DoD) - and authored by Willis H. Ware[17]. The report is widely considered to

13. Parisa Tabriz, "Keynote: Parisa Tabriz" (Black Hat USA 2018, 2018).

14. Ibid., Jeff Moss.

15. Allan Paller, "The Five Most Dangerous New Attack Techniques, and What's Coming Next" (RSA Conference 2018, 2018).

16. Steven Furnell and Nathan L. Clarke, "Guest editorial," *Information & Computer Security* 26, no. 3 (2018): 262–263, doi:10.1108/ICS-06-2018-0065, https://doi.org/10.1108/ICS-06-2018-0065.

17. Willis H Ware, *Security controls for computer systems*, technical report (RAND CORP SANTA MONICA CA, 1970).

be one of the most foundational works in Computer Security[18]. Beyond its seminal value, the story of how it came to be is of particular interest when considering the current state of Computer Science, especially in light of claims like Furnell's. According to Ware, the report was the result of water-cooler talk:

"..in the early 60's, some of [Ware and his colleagues] began to realize how heavily the military, the Air Force, and the DoD, were beginning to depend on computers, and correspondingly, to realize how heavily the country was beginning to depend on computers. We would talk amongst ourselves in the hallways at conferences and gradually there emerged a concern that we really ought to do something about finding out how to protect computer systems [...] because the country was so dependent on them."[19]

It is hard to imagine a more natural, human mechanism for the emergence of a feeling, in this case the identification of a need, than commonplace chats with colleagues. Indeed, the field which purportedly is only now coming to grips with its human elements, was birthed through that great common denominator of human interaction, small talk. Despite this admittedly abstract reading of the story, it serves to support two other, equally important facets of Computer Security, and Computer Science more generally: the degree of military influence on the field and the value of examining its history.

First, the Ware Report and its origin story serve to underline the strong interaction between US military structures like the DoD and the RAND corporation, and the computer-research community around the time the idea of Computer Security began being codified. This interaction, and its inherent 'securitizing' influence on the field of computing was explored by Thomas J. Misa in his 2016 article *Computer Security Discourse at RAND, SDC, and NSA (1958-1970).* Misa points out that the military's focus on national security was a strong component of the environment within which Computer Security emerged. Additionally, Misa writes:

"...the real measure of computer security is, in addition to robust technical concepts, the wider dissemination and embedding of computer security practices in government, industry, finance, communication, and the entire range of computer-dependent institutions."

This statement leads directly to the second important facet. The incredible resemblance between Misa's quantification of Computer Security, and the calls for cross-disciplinary investigations to bolster modern cyber security by the likes of Moss, Tabriz, and Furnell,

18. Thomas J Misa, "Computer security discourse at RAND, SDC, and NSA (1958-1970)," *IEEE Annals of the History of Computing* 38, no. 4 (2016): Misa provides evidence for this, partially in a list of famous CSS publications that refer to the report.

19. Willis H. Ware, *Oral history interview with Willis Ware*, Charles Babbage Institute, September 2003.

serves to highlight the essential benefits from considering the history of the field. Unquestionably, there is a great need for the technical, but there is also a need for situating the technical in the human.

There appears to be a slowly growing appreciation for this need. Top Computer Security publications and venues like the ACM Conference on Computer and Communications Security (ACM CCS), the IEEE Symposium on Security and Privacy (S& P), USENIX Security Symposium (USS) and Network and Distributed System Security Symposium (NDSS) which feature the cutting edge in technical innovation also often feature an article or two that address more human, or holistic, security concerns. The 2018 USS featured a talk by Susan Landau in which she described the most recent developments in what are often called the "Crypto Wars" : a series of often combative interactions between business, public-perception and the federal government over encryption.[20] USS 2018 also featured a relatively large amount of content related to privacy and anonymity. Perhaps exemplifying the current state of affairs is an article in S& P 2018 titled *Computer Security and Privacy for Refugees in the United States* by Lucy Simko et al.[21] The article reports difficulties refugees entering the US face with regard to technology, and uncovers previously unconsidered issues like the implicit cultural knowledge needed to set and answer the security questions required to authenticate a user who's forgotten her password. The presence of such implicit knowledge, while natural, forms a powerful mechanism for exclusion, a phenomenon central to our work. The authors suggest a number of improvements that could be made, of which only some are technical (e.g. the implementation and use of stronger encryption or the use of specific hardware and software).

Simko et al.'s article also serves to illustrate a final feature of the value of historical consideration. Difficulty assimilating into a new culture, and more generally the hardship associated with refugee status are in no way a digital-age phenomenon. After citing a "growing body of work considering diverse populations in computer security literature" , Simko points out that refugees are especially at risk in their asylum due to their likely difficulty with the native language, and a heavy reliance on the organs of state and NGOs. None of these issues are inherently digital, yet each may be affected by digital technology; computer-enhanced language and entrepreneurial training may hasten competence in both

20. Susan Landau, "The Second Crypto War - What's Different Now," in *27th USENIX Security Symposium (USENIX Security 18)* (Baltimore, MD: USENIX Association, 2018), ISBN: 978-1-939133-04-5, `https://www.usenix.org/conference/usenixsecurity18/presentation/landau`.

21. Lucy Simko et al., "Computer Security and Privacy for Refugees in the United States," in *2018 IEEE Symposium on Security and Privacy (SP)* (IEEE, 2018), 409–423.

areas. It is certainly reasonable therefore, as Simko does, to base a study of the digital in the human.

The importance of work like Simko's, evident minimally in its potential to produce tangible improvements in everyday lives of those displaced by violence, is readily apparent despite it not sharing many features with the technically-oriented articles it was published alongside. This movement away from the purely technical is one prong in a movement toward a more diverse, 'holistic' approach to cyber security. One might term this prong human-oriented holism. Another emerging idea of holism has been spearheaded by Shouhuai Xu, and based in the concept of a 'Science of Cyber Security'. Xu is known for his pioneering work on what he calls *Cybersecurity Dynamics*[22], an area around which he last year co-founded a conference called the *Conference on Science of Cyber Security*(SciSec). The 2019 SciSec website describes works published therein as "distinguish[ing] themselves from others by taking or thinking from a holistic perspective about cyber security, rather than a building-block perspective."[23]

On his website, Xu cites a 2008 conference sponsored jointly by the National Security Agency (NSA), National Science Foundation (NSF) and the Intelligence Advanced Research Projects Activity (IARPA) as having lead to a widespread recognition of the importance of "building a foundation for the science of cyber security."[24] The conference proceedings, referred to as the *NSF/IARPA/NSA Workshop on the Science of Security* (WSS), produced a report of the same name which clearly set out goals for the development of a science of security. Citing the gap in both theory and practice between a technology and its implementation (i.e. the RSA algorithm itself, and the need to keep a private key secret), the report goes on to suggest a blueprint for bridging that gap by pursuing a diverse range of studies, from exploring economic and biological metrics in addition to technical ones, to formal methods: in a word, holism. Over the last decade we have seen strides in that direction, as evidenced by works like those of Simko and Xu.

One particularly interesting feature of Xu's work is his notion of cyber security as a complex system resulting from the interaction of attackers and defenders.[25] In a 2014 paper titled *Emergent Behavior in Cybersecurity*, Xu outlined this idea, which codifies

22. Xu published a article with this title in the proceedings of the Symposium and Bootcamp on the Science of Security in 2014.

23. "The 2nd International Conference on Science of Cyber Security - SciSec 2019," 2019, `http://www.sci-cs.net/`.

24. Shouhuai Xu, "Cybersecurity Dynamics: A Foundation for the Science of Cyber Security," `http://www.cs.utsa.edu/~shxu/socs/`.

25. Shouhuai Xu, "Homepage," `http://www.cs.utsa.edu/~shxu/`.

in systems theory the potential for emergent behavior in the cyber realm which is not predictable by simply considering the individual components of the system; a system as complex as the modern cyber security landscape is more than the sum of its parts.[26] This at once explains Xu's notion of holistic cyber security, in opposition to the "building-block perspective", and provides us with a concrete connection to our proposed area of study.

From the proceedings of the 2008 WSS, a general understanding of the need to systematize, or universalize the field was developed. Holism was understood to be valuable, and its pursuit was called for. The past decade of Computer Security research can be seen as largely in keeping with this call. There has, for instance, been a fair amount of research devoted to creating taxonomies and topologies of threats and defenses which have sought both technical, and economic bases. Examples of such work include those of Harry et al.[27], Tuma et al.[28] and Bruijne et al.[29] Similarly, the work of Xu exemplifies the extremely formal end of this holistic spectrum, with much of his work revolving around systems theory and formal methods. Finally, at the other end of the spectrum are human-centric works like that of Simko, and those of Aurigemma et al.[30] and Levesque et al., the latter of which explicitly speaks to the importance of appreciating there being a "human-in-the-loop."[31]

A final feature of very recent activity in the Computer Security field should be addressed: the danger in 'silver-bullet thinking.' When Tabriz spoke at BlackHat 2018, she chided the crowd that "blockchain is not going to solve all of our security problems."[32] More optimistically, Rohit Ghai, President of RSA, in a talk he gave at the 2018 RSA Conference identified one of the recent successes in cyber security as "the end of the silver bullet fantasy."[33] This apparently spreading understanding that solutions to the problems of cyber security cannot come solely from a building-block, technology-centric orientation of the field is nearly definitional holism. The opposite of a silver-bullet approach to problem solving is one based on diversity.

26. Shouhuai Xu, "Emergent behavior in cybersecurity," *arXiv preprint arXiv:1502.05102*, 2015,

27. Charles Harry and Nancy Gallagher, "Classifying Cyber Events: A Proposed Taxonomy," *Journal of Information Warfare* 17, no. 3 (2018): 17.

28. Katja Tuma, Gül Çalikli, and Riccardo Scandariato, "Threat analysis of software systems: A systematic literature review," *Journal of Systems and Software* 144 (2018): 275–294.

29. Mark de Bruijne et al., *Towards a new cyber threat actor typology*, technical report (Delft University of Technology, 2017).

30. Salvatore Aurigemma and Thomas Mattson, "Effect of long-term orientation on voluntary security actions," *Information & Computer Security* 27, no. 1 (2019): 122–142.

31. Fanny Lalonde Lévesque et al., "Technological and human factors of malware attacks: A computer security clinical trial approach," *ACM Transactions on Privacy and Security (TOPS)* 21, no. 4 (2018): 18.

32. Tabriz, "Keynote: Parisa Tabriz," 26:30.

33. Rohit Ghai, "Cybersecurity Silver Linings" (RSA Conference 2018, 2018), 4:29.

Such diversity is improved by considering how human the origins of the field of Computer Science and Security are, as Misa did. It is improved by a broad, but singularly focused research orientation, as called for by the 2008 WSS, and as pursued by the likes of Simko, Xu, and Bruijne. It is further enhanced when researchers consider pre-digital phenomenon, such as refugees and the emergent properties of complex systems not as entirely new in their digital forms, but as the result of an interaction between the pre-digital form, and digital technology. One such phenomenon that, to the best of my knowledge, has yet to be examined within this frame is securitization; a concept neither new, nor intrinsically digital, yet prevalent in the cyber world.

In light of the ever increasing speed of technological development, and the similarly quickening pace of product development[34] often capable of creating new spaces (i.e. social media platforms, wearables, etc.) it seems more pressing than ever to consider securitization. Like Xu, I propose to study emergence, but unlike Xu's formal methods and complex systems theory approach, I propose to undertake it using the tools of historical exploration, grounding my investigation not in math, but in people.

2.2 Business, and Engaging Self Interest

When Jeff Moss spoke to the clash of security models between the political and business worlds, he touched upon a story which has had a powerful impact on the modern state of Computer Security. From its outset, the field has been driven by the interaction between the two worlds. In the post-WWII era, there appeared a military-oriented, fairly top-down research and development environment. Then, as information and computing technology became more and more widespread, classically economic drivers began to exert themselves on the state of information systems leading to the development of the first ever "security software products industry" .[35] Following the emergence of the security software field, events like the Morris worm served to draw public attention to computer security, reinforce a monetary framing of the problem, and provoke non-military elements of the political world into taking regulatory action.

34. Benoit Dupont, "Cybersecurity futures: How can we regulate emergent risks?," *Technology Innovation Management Review* 3, no. 7 (2013): Dupont points out that "faster innovation cycles" negatively incentivizes a security focus during development.

35. Jeffrey R Yost, "The Origin and early history of the Computer Security Software products industry," *IEEE Annals of the History of Computing* 37, no. 2 (2015): 46–58.

Today, this interaction is as powerful as ever. Civilian political structures are constantly working to maintain an appropriate regulatory environment in the face of the ever increasing pace of technological development. Concurrently, their military cousins strive constantly to maintain a competitive edge and align pre-digital notions of security with modern technology. At the same time, the constant interaction between producers and consumers, collectively the business world, jointly interact with that political structure. This compound dialectic, which parallels the developing appreciation for holism, begins in the 1940s.

In the aftermath of WWII, the non-Soviet Allies could see the writing on the curtain, and the US feared that the incredible speed with which they had been able to develop new technology and weapons during the war would wane during peacetime and leave them vulnerable.[36] The US Air Force (USAF), newly in charge of the most destructive weapons ever built, wanted to prevent what they perceived as a potentially deadly movement away from military research and development. With the Manhattan Project fresh in their memories, top USAF leadership envisioned and established the RAND Corporation: a civilian research group devoted to military projects, whose only customer was - initially - the USAF. Today, RAND exists as a non-profit corporation, and serves customers ranging from non-US government agencies, to other nonprofits.[37] In light of the RAND corporation, under whose auspices Willis Ware published his now famous report, Moss's statement suggesting an emerging clash of models seems odd.

Skipping ahead a few decades from the RAND corporation's highly political, military origins, we can see the growing influence of business on the field in the early years of what is often termed the security software market.[38] IBM, which had become dominant in computing during the same post-WWII era that produced RAND was, unlike RAND, a for-profit business. Part of what fueled IBM's long-term success and profitability in the information technology industry was its culture of listening to the customer,[39] and by the late 1970s those customers were becoming concerned with security. Already in 1972, time-sharing was becoming the dominant form of computer access and many resources were being invested in network research.[40] This had the somewhat unexpected effect of

36. Alex Abella, *Soldiers of reason: The RAND corporation and the rise of the American empire* (Houghton Mifflin Harcourt, 2009).

37. "RAND at a Glance," RAND at a Glance, `https://www.rand.org/about/glance.html`.

38. Yost, "The Origin and early history of the Computer Security Software products industry."

39. Ibid.

40. *Computer Networks - The Heralds Of Resource Sharing*, International Conference on Computer Communications, 1972.

massively enlarging the potential attack surface of computing centers. Where before physical security and aggressively vetting a very small number of trusted managers had served to mitigate many, if not most potential attacks on computing infrastructure, now potential threats did not necessarily need to gain physical access.

Despite an apparently emerging market for non-governmental security software, IBM's earliest attempt to produce such a system, what we might now generally term some form of *access control*, was in response to a large government contract and resulted in a system called the *Resource Security System* (RSS).[41] Though RSS was ultimately unsuccessful as a product, the combination of the attempt, and IBM's perception of the emerging market for security software lead to their producing *Resource Access Control Facility* (RACF); their first commercially successful security software. Tellingly, a core lesson IBM drew from the RSS failure, was that the military-level security its contract called for came at such a high-efficiency cost that businesses, beholden to their profit margin, often preferred no security over the overhead introduced by a high-assurance system. By 1974, having determined that most of their potential customers were only interested in protecting 10-20%[42] of their data - what Moss would call their "Golden Eggs"[43] - they designed RACF to provide a variable amount of protection. IBM's customer orientation and business' profit-model resulted in the first widely marketed security software product being one which followed the opt-in model of security, rather than the high-assurance security model favored by the governmental actors.

By the late 1970s, two other similar products vied for the same market. In particular contrast to the opt-in model of IBM's RACF, SKK Inc.'s[44] ACF2 product featured a 'protection by default'[45] design. Interestingly, according to the Barry Schrager, the 'S' of SKK, ACF2's market share was boosted by two governmental acts, one civilian, and one military. On the civilian side, the passage of the 1977 Foreign Corrupt Practices Act (FCPA) resulted in any business operating internationally being required to secure their computerized financial data. Around the same time, the CIA bought ACF2, hoping to determine how breakable it was. After finding an exploitable flaw, they recommended ACF2 to their international counterparts (like MI5, and the Australian DOD), resulting in yet more business for SKK Inc.[46]

41. Yost, "The Origin and early history of the Computer Security Software products industry."
42. Ibid.
43. Tabriz, "Keynote: Parisa Tabriz," Jeff Moss.
44. SKK Inc. was an American startup originally consisting of Barry Schrager, Eberhard Klemens and Scott Krueger
45. Schrager, *Oral history interview with Barry Schrager*, Charles Babbage Institute, 2012.
46. Ibid.

The story of IBM, SKK Inc, the CIA, congressional acts, and the early security software market serves not only as a defining example of the complex interaction between business and political structures over computing, but is also suggestive of the inherent difficulty in advancing Tabriz' culture of defense. Clearly, systems which require security to be considered at each step in their design, and which emphasize protection by default are systems embodying a defensive culture. However it is equally clear that such a culture is somewhat antithetical to a for-profit software development cycle. Further hampering the development of such a culture is the fact that a defensive system must be paid for up front, but its value-adding potential requires that there are actual attacks that it deflects. Compared to, for example, investment in improved factory tooling, the value of which one can calculate down to the cent, investment in defense is a gamble. Despite what has become an almost constant stream of cyber-incident stories in the news, this basic feature of continuous defense still acts as a force against the widespread adoption of a defensive culture. With this in mind, it is no surprise that in the 1970s there was considerably less enthusiasm for paying for defenses against what most people considered to be incredibly rare attacks.

It was in this climate that the first highly structured attempt was made to develop a formalized notion of computer security intended to incorporate both business and political interests. In 1978, Paul Walker had become attached to the Office of the Secretary of Defense (OSD), and the DoD spearheaded this formal exploration of how to meet security goals by establishing the Computer Security Initiative (CSI).[47] Beginning in the same year, the CSI brought together representatives from government, government-sponsored research groups, and private industry including IBM.[48][49] Largely directed by government actors, the CSI can be viewed as an attempt to formalize security standards in the face of an emerging concern over system security, like those raised by the *Ware Report*. One result of the initiative was the now famous Orange Book. First released in 1983, the Orange Book, officially the *Trusted Computer Systems Evaluation Criteria* (TCSEC), established a framework by which security products, like RACF could be evaluated. However, as Jeffrey Yost writes, "Computer manufacturers often neglected to invest in developing systems to high TCSEC levels to supply to the federal government... ."[50] There was simply no

47. Steven B Lipner, "The birth and death of the orange book," *IEEE Annals of the History of Computing* 37, no. 2 (2015): 19–31.

48. Ibid.

49. Peter S Tasker, "Trusted computer systems," in *1981 IEEE Symposium on Security and Privacy* (IEEE, 1981), 99–99.

50. Yost, "The Origin and early history of the Computer Security Software products industry."

incentive to develop extremely secure systems if only the federal government wanted them while most companies remained apathetic. By 1987, the NSA's continued insistence that the Orange Book was broadly applicable outside of national-security oriented operations caused industry insider Robert Courtney to go so far as to call it "an excellent example of the inflexibility and the intellectual slovenliness of the bureaucratic mind."[51]

Despite the arguably limited success of the CSI's Orange Book from the perspective of broadly improving the security of vendor-produced security softwares and operating systems, CSI certainly represented closer interaction between the business and political worlds. What had yet to be truly engaged however, was the great capitalist driver of self-interest: until the profit margins of companies were significantly affected by computer security, or lack thereof, companies remained resistant to rebalancing their culture, even slightly, toward defense.[52] Over the course of the 1980s, appreciation of this driver would grow steadily.

This growth is perhaps best evidenced by two events: the 1984 passage of the Computer Fraud and Abuse Act (CFAA), and the 1988 Morris Worm incident - the first jury test of the CFAA. In keeping with the paradigm we observe in all of our events, the passage of the CFAA was due in no small part to the public concern generated by the 1983 release of the movie *WarGames* in which a teenaged computer enthusiast nearly triggers nuclear war from his bedroom.[53] Following its release, press coverage of the movie focused on the potential real-world feasibility of the plot as public attention was suddenly focused on the emerging Internet. Foreshadowing modern calls to consider the security implications of the 'human-in-the-loop', when asked in an interview on ABC whether or not a *WarGames*-like scenario was possible, then NORAD spokesman General Thomas Brandt tried to quell fear by stating that a "man is in the loop" during all nuclear decisions.[54]

We will explore the second of these events in more detail in chapter 5, but for now one feature of Morris' Worm is chiefly important: it powerfully and publicly demonstrated that computer security was a serious, tangible problem, and that there was a real dollar cost to ignoring it. Where *WarGames* was theoretical, Morris' worm was concrete and expensive. The US General Accounting Office (USGAO) - which was commissioned by

51. Robert H. Courtney Jr, "Contemporary data security: A leadership vacuum.," *COMP. SECURITY J.* 4, no. 2 (1986): 7–16.

52. Adam Smith, "An inquiry into the nature and causes of the wealth of nations: Volume One" (London: printed for W. Strahan; / T. Cadell, 1776., 1776), 9.

53. Stephanie Ricker Schulte, "'The WarGames Scenario' Regulating Teenagers and Teenaged Technology (1980—1984)," *Television & New Media* 9, no. 6 (2008): 487–513.

54. ABC News, "World News Tonight," *ABC*, July 8, 1983, `https://archive.org/stream/ABCNews19781979/ABC%20News-1983-1984-B-e.txt`.

Congress to investigate the impact of the event - estimated that the worm caused dollar losses of up to $10 million.[55] Such incidents, which have only gotten more common and more expensive, serve to continually engage the self-interest of the business world.

If we consider Morris' Worm a proof-of-concept event in terms of a culture of defense requiring the engagement of self-interest, Microsoft's experience with its enterprise customers around the turn of the century would represent the release of a long-term support version. In her book *Listening In: Cybersecurity in an Insecure Age*, Susan Landau quotes Steven Lipner, who in 2001 was Microsoft's Director of Security Assurance, as saying "By the end of 2001, no Microsoft executive could have any conversation with any enterprise customer about anything but Microsoft's bad security."[56] Understanding that Microsoft's previous business model of prioritizing features and time-to-market over other concerns was starting to cost the company money, Microsoft undertook a massive overhaul of their development process. The result was generally improved security, and a security-oriented development cycle that has since become an industry standard.[57]

What we see when we consider this history of the field are a series of developments which each uniquely adjusted the relationship between the political and business worlds over computer security. In its earliest stages, WWII era strategic thinking resulted in the incredibly top-down approach of setting up the RAND corporation, designed to keep technological progress under the auspices of the federal government and military. Subsequently, the emergence of the security-software market saw organs of government try to incorporate greater input from non-governmental interests, resulting in organizations like the CSI. However, despite business input, the inertia of decades of national security oriented thinking resulted in fairly top-down, and therefore impotent solutions like the requirements of the Orange Book.

By the end of the 1980s, theory-first approaches to computer security began giving way to a more pragmatic, bottom-up force which grew out of an understanding of the insecurity of increasingly networked systems, increasing public engagement on the topic, and a dawning realization that poor computer security could have real dollar costs. Early manifestations included the passage of the CFAA and the establishment of a US national

55. JB Hoy et al., *Computer Security: Virus Highlights Need for Improved Internet Management*, technical report (GENERAL ACCOUNTING OFFICE WASHINGTON DC INFORMATION MANAGEMENT AND . . ., 1989).

56. Susan Landau, *Listening In: Cybersecurity in an Insecure Age* (Yale University Press, 2017), 51, quoting from an interview she conducted with Steven Lipner in December of 2016.

57. Ibid., 51.

Computer Emergency Response Team (CERT) in the wake of the Morris Worm.[58] By 2001, this force was powerful enough to dramatically alter the behavior of one of the era's largest technology companies.

If we now reconsider Moss's statement on the clash of political and business models, we see that it is only odd if taken to mean that the interaction is new. Clearly that is not the case. If however we interpret it as an appreciation on Moss's part of a new phase in the interaction, one marked by the nation-state actors, Facebook and Russian trolls, it rings true. Considering the theoretical, top-down approach as rooted in military and political structures and the pragmatic, bottom-up approach as rooted in business and public perception presents an attractive parallel to the growing appreciation for holism emerging from within the field of computer security. Like the diversity in approaches taken by the likes of Xu and Simko collectively represent the past decade's increasingly holistic orientation, so too does the increasing appreciation for a dialectic interpretation of the business and political worlds. Since RAND, the trend has been toward more cooperation and interaction between the two, not isolationism. Finally, like holism, this interaction is neither new, nor inherently digital, yet its character has undergone change in the digital age. Just as this feature of holism suggests the benefits of considering a phenomenon like securitization through updates in the forms of computing technology, so too does the political-business dialectic.

58. Hoy et al., *Computer Security: Virus Highlights Need for Improved Internet Management*.

3

Concepts

3.1 Commons

In 1968, Garrett Hardin gave an address to the American Association for the Advancement of Science, titled *The Tragedy of the Commons*[59] which drew directly from a series of lectures given by William Forster Lloyd in 1833[60]. Hardin popularized the phrase 'Tragedy of the Commons', as referring to a situation where a common resource, like a shared grazing pasture (a commons), is degraded over time by the self-interested use of individuals. The tragedy, in Lloyd's words, "is that the universal distress fails to suggest to individuals any motive for moral restraint."[61] While both works focused primarily on 'population control' with regard to the carrying capacity of the world's natural resources, the concept has come to be broadly applied. For our purposes, the concept appears to have an integral relationship with the emergence of notions of security.

The original example provided by Lloyd revolves around a shared grazing space for cows. While the number of cows being grazed on the commons remained less than a certain, critical mass, the commons was naturally able to sustain itself, just as a wild grazing space could naturally support a small number of herbivores indefinitely. However at some point, as the number of people grazing their cows grew, or as those individuals began to graze more than a single cow each, the capacity of the commons was surpassed, and its ecosystem began to fail. Because the marginal cost of each additional cow was shared by the entire community, while the benefit accrued solely to its owner, there existed a positive economic incentive for individuals to make greater and greater demands upon

59. Garrett Hardin, "The tragedy of the commons," *Science* 162, no. 3859 (1968): 1243–1248.

60. William Forster Lloyd, *Two Lectures on the Checks to Population: Delivered Before the University of Oxford, in Michaelmas Term 1832* (JH Parker, 1833).

61. Ibid.

the commons. Fatalistically, this resulted in the tragic death of the commons. However, if rules were agreed upon which governed its use, and if all individuals obeyed those rules, a certain number of cows could be grazed there indefinitely. In order to prevent the extremely harmful death of the common resource, rules needed to be adopted and enforced to govern its usage.

Before considering the afore alluded to abstractions of this idea which make the tragedy of the commons useful for our purposes, it is important to consider the ways in which digital and non-digital structures and communities do and do not conform to the concept of a commons. This is perhaps best captured by Mark Raymond whose 2013 article titled *Puncturing the Myth of the Internet as a Commons* argues convincingly that the Internet is not a true commons.[62] Chiefly, it is valuable to note that the fundamental digital-structures within which most of our chosen events take place are not well captured by the definition of a pure commons. The Internet is, for instance, in many places guarded by authorities who selectively permit their users access.[63] We will consider these issues more extensively in section 4 as we explore the case of the passage of the FCRA, but for now we will focus on the element of tragedy, which we will work to demonstrate quite accurately fits into each of our chosen events, and is a core component of securitization. While the airline industry was clearly not a commons, its pre-9/11 state was much closer to a commons than its post 9/11 state, and the transition was defined by tragedy.

Following from such a focus on the tragedy, it is also valuable to consider the different ways in which this basic mechanism might present. For instance, upon consideration, it is reasonable to think of such events as losses of innocence. As aforementioned, 9/11 represented a tragic, collective loss of innocence. Where before we had been happy to ignore what with hindsight appear glaring similarities between jet liners and cruise missiles, the after state is characterized by constant painful remembrance of our lost ignorance. In the era of Morris, there was already potentially valuable data available via machines connected to the Internet. Yet while within the Internet community, and especially within its military component there was already a serious concern over the Internet's security, when Morris made the front page of the New York Times, he put the final nails in the coffin of our then-collective conceptualization of the Internet as an innocent, open space.

62. Mark Raymond, "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*, 2013, 53–64.

63. Lena L Zhang, "Behind the 'Great Firewall' Decoding China's Internet Media Policies from the Inside," *Convergence* 12, no. 3 (2006): 271–291.

Considering this interpretation of both 9/11 and the Morris Worm, it seems reasonable to consider some form of tragic realization a component of securitization. Throughout the following sections, we will explore this theme as it appears in our chosen events. For instance, Morris' worm laid bare the potentially tragic nature of what was up until that point, a very open, and fairly unregulated Internet ecosystem. Michael van Eeden's multi-user dungeon (MUD) in Amsterdam's Digital City was originally a truly utopian, wholly unregulated, free space. It wasn't until a single user's lack of moral restraint threatened the entire system's existence that an authority was established.[64]

3.2 Exclusion

The paradigm of exclusion appears consistently alongside emergent security. Through our case studies, we will see it take a number of different forms, and act upon different components of events; whether as an impetus or a reaction or both. For instance, in the FCRA case, the threat to the commons was due to the natural emergence of exclusion in a relatively free market. In response, fine-grained exclusionary mechanisms were imposed on that newly created market, functionally securitizing it. In this way, emergent exclusion resulted in a broad concern over potential abuse, and exclusionary action was taken. It appears fundamental to the value of the FCRA case to appreciate the difference between these two exclusionary actions. When it emerged naturally yet unexpectedly out of a growing market need for social credit information, and given a zeitgeist increasingly concerned with dehumanization through computerization, exclusion caused concern, and cries for regulation. However with the passage of the FCRA in 1970, an act which excluded a number of predatory and illiberal practices, exclusion was greeted with enthusiasm and praise. We will explore this idea in more detail when discussing the FCRA in more detail in section 4, but we present it here to underscore the abstract expansiveness of exclusion.

The passage of the FCRA also demonstrates one common form of reactionary exclusion: the establishment of enforceable rules. As the US Congress is tasked with creating laws by which all US citizens, both consumers and providers of credit information, must obey, they are well positioned to make rules governing the interaction between the two. Further, as Congress' direct authority is constituted by Federal power, such as that wielded by the FBI and DEA, any regulations they pass can immediately be enforced without delegation

64. Michael van Eeden, *Interview*, June 25, 2018.

outside their general organization; in this case the US Federal Government. Such an overarching structure provides a ready-made mechanism for enacting securitizing exclusion. However as we'll see in more recent events, such a structure is not always available, and in such cases exclusion may be achieved through alternative means.

For instance, when such a situation occurs between nations, as happened in Estonia in 2007, there is no global power structure with the same potential authority as there is within a country. There is therefore no possibility to enact exclusionary measures through those means, and others must be considered. Estonia combined a digital-age technical response with a more classical strategic effort. On the technical front, they diligently set about improving their ability to exclude bad actors from their digital infrastructure. At the same time, they also more closely tied themselves to NATO, whether intentional or not, by jointly choosing to establish the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn. The centre, which now runs sophisticated cyber-war games, inherently excludes non-NATO members, the great historical example of which is Russia.

Finally, our most recent event represents yet another seemingly unique organization of the exclusionary paradigm. Few things are more antithetical to the basic principles of democracy than exclusion, and so when those principles were perceived to be attacked by the Russian state in the 2016 US presidential election, a new front was opened, one that has yet to be fully explored. While the jury, both American and International, is still quite clearly out on how to deal with this emerging problem, the attempts to improve the identification and removal, or exclusion, of foreign agents from social media platforms has been one of the only concrete steps taken thus far. Like the FCRA model, the US appears to be enacting exclusionary rules. However, like the Estonian model, there are components to the issue which are not within the power of a single nation to regulate. Today's great emerging securitization appears to be that of the democratic process itself.

3.3 Cyber Security

In October of last year, political scientist Henry Farrell and "security technologist"[65] Bruce Schneier authored an analysis of the current state of cybersecurity with respect to foreign meddling in basic democratic processes.[66] Their analysis, in keeping with their

65. Bruce Schneier, "About Bruce Schneier," `https://www.schneier.com/blog/about/`.

66. Henry Farrell and Bruce Schneier, "Common-Knowledge Attacks on Democracy," *Berkman Klein Center Research Publication*, nos. 2018-7 (2018).

backgrounds, explored the potential unification of the hitherto disparate orientations of national security and computer security. They suggest one way to achieve this might be to consider states as information systems which immediately leads to a mingling of the terminologies of the two fields. Traditional cyber security terms must be evaluated in terms of non-cyber systems. As our work involves similar cross framing, it is useful to consider how some of these terms and the ideas they represent cross boundaries. Specifically useful from our point of view are the widely used terms *attack surface* and *threat model.*

A recent NSA-sponsored research project which explored the use of the term attack surface in computer security literature determined that there is a considerable amount of variety in its use. As such, they suggested that for the purpose of reducing friction during scientific discourse, a definition of the term should be chosen in keeping with the characteristics of the object of study.[67] The authors support this position as having been derived from what they consider the canonical definition of attack surface, that of Howard et al., who provided three dimensions upon which to gauge a surface's size.[68] The first dimension captures the number of targets or routes of access to targets. The second reflects the permissive nature of the means of communication and rules of communication available between an attacker and her target. Finally, the third dimension captures the relative value of each potentially compromised target, or component, both innate and with respect to potential lateral access. Collectively, the greater the available means of access to potentially vulnerable parts of a system, the greater the attack surface.

Armed with this definition, let us briefly consider two instances of securitization, each representing very different systems, through the lens of their attack surfaces. First, on our canonical 9/11, as it was the airline industry and its associated processes that were securitized, we'll consider their combined attack surface. With the benefit of hindsight, it is possible to see that the vulnerable systems were the airplanes themselves, and any auxiliary processes which could provide or enhance access to them. These range from, most broadly, the airports which control passenger access to the planes, to the doors which segregate passengers from pilots. Included in that range are all of the humans, protocols and devices designed to screen passengers and baggage, and manage access to the planes themselves. In this way, airports, airlines and their planes represent a very technology-oriented attack surface, one which is closely related to the 'stuff' of airplanes.

67. Christopher Theisen et al., "Attack surface definitions: A systematic literature review," *Information and Software Technology* 104 (2018): 94–103.

68. Michael Howard, Jon Pincus, and Jeannette M Wing, "Measuring relative attack surfaces," in *Computer security in the 21st century* (Springer, 2005), 109–137.

Additionally, due to the airline surface being so technology heavy, the fact that humans still play such a large role in its surface strongly reinforces the need for holistic approaches to security.

A very different type of system was attacked during the 2016 US presidential election. In this case, there was not a physical computer or object to protect, or a cockpit-like space to secure access to. There was public opinion, complete with its innumerable means of being accessed and attacked. As Farrell et al. hold, the target in 2016 was the "common political knowledge" of the US electorate, by which they mean that knowledge, like the expectation that election results will be universally respected, upon which the democratic process stands.[69] Here, there are no doors to be reinforced, or metal detectors to be installed, yet by virtue of a target being identifiable, and attacked, a surface must exist. Following from Howard et al.'s definition, that surface must include all means of access to public opinion, of which social media is the glaringly obvious modern vector. Such disparate mechanisms as airport metal detectors and Twitter, unified, serve to underscore the value of the attack surface concept in the pursuit of a better understanding of modern securitization.

As our work integrally involves considering security as a diverse and holistic pursuit, including the notion of the 'human-in-the-loop', it is useful to consider the enormous attack surface of a human. Abstractly, a human must not only maintain their biological processes by consuming nutrients and expelling waste, but also maintain whatever endeavors they have undertaken. In the context of much of the world, some of those endeavors approach the criticality of biological maintenance in terms of sustaining life. Such pursuits include earning a wage with which to acquire the means of subsistence, maintaining some level of social status, and procreation. Finally, a human is also vulnerable to physical threats ranging from viral infection to assault. Fundamentally, everything in the human experience capable of causing pain constitutes an individual's attack surface. Considering our definition in terms of a human therefore lays bare the truly awesome task of achieving a highly secure state, and underscores the value of considering a variety of systems from the perspective of their attack surfaces.

As fundamental to security as understanding what's vulnerable and by what means, is understanding who may seek to exploit those vulnerabilities, and why. Where strictly considering an attack surface nominally supposes an all powerful adversary in that all conceivable vulnerabilities are considered, no matter how difficult or expensive they may be to find and exploit, a threat model seeks to provide insight into what is likely to be

69. Farrell and Schneier, "Common-Knowledge Attacks on Democracy."

attacked, and what characteristics a likely attack would feature. An abstract, widely shared definition of threat modeling comes from Uznov and Fernandez: "Threat modeling is a process that can be used to analyze potential attacks or threats..."[70] A more succinct and application-friendly definition, set forth in a widely cited 2009 article by Cardenas et al. reads "the goal of defining a threat model is to formalize our perceived *risk*."[71]

One feature of securitization is the updating of threat models, or a reevaluation of risk. This is particularly clear when the development and deployment of a new technology is not accompanied by an updated threat model which takes that new technology into account. Often, security incidents which occur within this gap serve to jumpstart the securitization process and kick off the update process. Examples of this are manifest. For instance, French military doctrine just prior to WWI favored *cran* and *elan* guts and courage, as underpinning an almost exclusively offensive strategy. Despite incredible displays of both on the part the French soldiery, their threat model was one which seemed to largely ignore the potentially effective use of the then still relatively new machine gun.[72] Quickly, the French updated their model.

Another, more modern example plays out in the aforementioned thriller *WarGames*, in which the powers that be could not imagine that a lone teenager might pose a real risk to their incredibly sophisticated, multi-million dollar, nuke-controlling computer system. After having seen the movie, Ronald Reagan famously asked the joint chiefs "Could something like this have happened?" to which they replied, "Mr. President, the problem is much worse than you think."[73] Indeed, as we will explore in more detail in section 5 a core feature of the securitizing effect of the passage of the CFAA and subsequent Morris Worm incident was the way they forced the update of computer threat models. In 1914 it was the machine gun; in 1983 it was a movie about a bored teenager.

70. Anton V Uzunov and Eduardo B Fernandez, "An extensible pattern-based library and taxonomy of security threats for distributed systems," *Computer Standards & Interfaces* 36, no. 4 (2014): The assertion that their definition is widely held comes from Xiong, W. and Lagerstrom, R., 2019. Threat Modeling-A Systematic Literature Review. *Computers & Security*.

71. Alvaro A Cardenas, Tanya Roosta, and Shankar Sastry, "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems," *Ad Hoc Networks* 7, no. 8 (2009): 1434–1447.

72. Barbara Wertheim Tuchman, *The Guns of August* (Macmillan, 1962).

73. Fred Kaplan, *Dark Territory: The Secret History of Cyber War* (Simon / Schuster, 2016).

4

Passage of the FCRA

4.1 Computerization and Looming Dehumanization

Post WWII America was characterized, in part, by an aggressive pursuit of the 'American Dream', a dream that was growing increasingly expensive. Automobiles for instance, had become powerful symbols of success, but had very high sticker prices. At the same time, Americans were fresh off a seemingly universal international victory, and optimism reigned. Under these conditions, the practice of purchasing on credit exploded[74][75]. In this climate, an existing, but undeveloped network of consumer credit information brokers expanded rapidly, transitioning from an ad-hoc network of highly localized and sector-specific agencies which may have done little more than compile 'blacklists' of unreliable payment makers, into something we might today recognize as a credit reporting agency (CRA). Specifically, from newspapers and by other means, they began to collect consumer information ranging from marriage status and job promotions to arrest records.[76] They also began to cross sectors and grow outside their original communities: where once an agency may have specifically collected basic information in a single town or county for use strictly by retailers, that agency may thereafter have begun collecting more information, selling it to both retailers and banks, and been expanding to the state level[77] By 1955 this trend was clear, and was depicted in a congressional report by the Senate subcommittee on Antitrust and Monopoly.[78]

74. Nigel Watson, *An abridged version of the Experian: the story so far*, Experian Inc. 2013.

75. Andrea Ryan, Gunnar Trumbull, and Peter Tufano, "A brief postwar history of US consumer finance," *Business History Review* 85, no. 3 (2011): 461–498.

76. Mark J Furletti, "An overview and history of credit reporting," *Available at SSRN 927487*, 2002,

77. Ibid.

78. United States., *Consumer credit industry: hearings before the Subcommitte on Antitrust and Monolpoly of the Committee on the Judiciary, United States Senate, Ninetieth Congress, first session, pursuant to S.*

By 1960 this practice was so well established that it became an international model. In a New York Times article published in November of that year, the then chairman of the National Commercial Bank of Scotland is quoted as saying: "We hope to get to the stage they have reached in the United States, where everybody has a credit rating."[79] It was in this climate that concerns over how consumer information was used, and to what extent a consumer should have control over their data began to surface. A 1968 Times article captures well the state at the closing of the decade. Fittingly titled *Senate Investigators Examining Reports of Faulty Credit Ratings*, it quotes a federal investigator who sums up consumer sentiment toward CRAs saying "people are frightened."[80] The article also cites several horror stories, where people's lives were tragically altered by erroneous, in some cases even callous, administration by the agencies. As the title of the article suggests, in 1967, the Senate subcommittee on Antitrust and Monopoly held public hearings on the matter, in response to what then chairman Phillip A. Hart described as "complaints" his subcommittee had received.[81] The hearings were to determine if new legislation was needed, and consisted of experts from across the banking, lending and credit reporting industries testifying to the state of the sector. In response to growing public concern over perceived CRA apathy toward individual rights, it was determined that action should be taken.

A year after the hearings, in a similar but separate action, congress passed the Consumer Credit Protection Act (CCPA). The CCPA targeted lending practices deemed unfair, including the garnishment of wages without adjudication, and deceptive loan sales tactics.[82] Two years later in 1970, congress passed the Fair Credit Reporting Act (FCRA), a direct result of the 1968 hearings, and incorporated it into the CCPA as additional titles. The FCRA represents one of the earliest legislative attempts to protect people from unfair use of their personal data.[83] It achieved this through the introduction of enforceable rules which excluded previously legal practices which a majority of Americans had come to perceive as immoral. Functionally, the FCRA accomplished this by enumerating what rights

Res. 26. (Washington: U.S. Govt. Print. Off., 1967), 3 v., `//catalog.hathitrust.org/Record/008515191`.

79. New York Times, *British Finance Companies Map Credit Ratings for Consumers*, November 29, 1960.

80. New York Times, *Senate Investigators Examining Reports of Faulty Credit Ratings*, May 23, 1968, 12.

81. States., *Consumer credit industry: hearings before the Subcommitte on Antitrust and Monolpoly of the Committee on the Judiciary, United States Senate, Ninetieth Congress, first session, pursuant to S. Res. 26.*

82. United States., *Consumer Credit Protection Act and Truth in Lending Act* (United States. Congress, May 1968).

83. Landau, *Listening In: Cybersecurity in an Insecure Age*, 14.

consumers had with regard to their personal data, established limits on the use of their data, and provided avenues of recourse in the event of misuse or error.[84]

The 1970s saw CRAs aggressively adopt computer technology to aid their data-heavy activities. This lead to an increasingly consolidated field, driven by the immense gains to be had in such a data-oriented environment through computerization. As computerization was extremely capital intensive, only the largest of the agencies could quickly adopt the technology, and those soon became the dominant players.[85] However that decade of computerization proceeded the early securitization of the industry, an exploration into the causes of which will flesh out our use of the concepts of the commons and exclusion, and reinforce the technology-agnostic nature of securitization.

4.2 Commons Scaffolding and Securitization

As alluded to in the section 3.1, the definition of a pure commons is so narrow as to rarely apply in full to real-world situations. For instance, given the ubiquity of property rights in many places today, it is unusual to find anything, physical, intellectual or otherwise, for which no ownership, or at least rights of access, are defined. Similarly, issues of scale have hampered our ability to empirically determine whether something may in fact be used by a large population without consequence. However these superficial issues have not diminished the concept's utility. The commons apparent in this case provides an excellent opportunity to explore the utility of the concept, and to refine the idea in terms of securitization. First, we will consider what existed before the rapid growth of the CRA industry in the 1960s.

Over the course of the 1950s and 1960s, using the vocabulary of the free market, an industry naturally emerged to fill an ever increasing need to make wise lending decisions. The natural predecessor to such a system can be found in any community where information having to do with an individual's character is spread through any means: nearly every community conceivable. We will abstractly consider the good being exchanged as social-credit information (SCI), which captures the wide variety of potentially useful information, from financial to demographic, available about an individual. The word 'reputation' captures this nicely, as you may easily imagine someone's reputation preventing them from obtaining a loan from a bank, causing people to avoid that individual after they have

84. Furletti, "An overview and history of credit reporting."
85. Ibid.

been drinking, or to deny them access to community resources. Modern instances of such systems can be found in peer-to-peer services from Ebay to Uber. Both use reputation systems to help users make informed decisions about who they conduct business with in a fashion designed to emulate the organic 'word-of-mouth' systems present in human communities. They facilitate the exchange of SCI.

In their infancy, the extremely local, sector-specific credit reporting agencies still behaved much as the natural human system they were augmenting did. However, driven by the explosion of credit seeking in the 1950s and 1960s, this accepted, public process of assigning potentialities based on observed actions was codified and developed. What had previously been public information, i.e. the 'words'-of-mouth, was increasingly replaced by higher quality, professionally curated information. As the quality of CRA dossiers increased, so did their value, and correspondingly, their price. This augmentation transformed the SCI market into a pay-to-play market; no longer could everyone benefit freely and equally from its existence, and the resulting information asymmetry lead to abuses[86]. These abuses, and perceived abuses lead to a public outcry for oversight resulting in the 1968 Congressional hearing, and the subsequent passage of the FCRA.

Having established this transition, it remains to consider it as it relates to the tragedy of the commons, and to do this requires first distinguishing a commons from a pure-public good. A pure-public good is one which is both 'non-excludable' and 'non-rivalrous'; excluding would-be users is effectively impossible, and use by one individual doesn't reduce the benefit another may reap from its use (e.g. national defense). A club good, generally considered a type of 'impure' public good, is similarly non-rivalrous, but excludable in that an individual may be prevented from making use of the good (e.g. a toll road). Similar to a pure-public good, a commons is a resource from which users cannot be excluded, and which is non-rivalrous up to a point. The tragic nature of the commons only reveals itself when the resource's carrying capacity has been exceeded, at which point it becomes rivalrous due to individual consumer's lack of moral restraint, and begins to degrade. In this way, the tragedy of the commons arises directly out of the transition of a resource from pure-public toward private.

In terms of the passage of the FCRA, it seems reasonable to consider the resource in question to be a financially-oriented, social-capital market (SCM) which facilitated the trade of SCI. SCMs as they existed before the CRA boom of the 1950s and 1960s existed as public goods, the atomic units of which were produced passively and consisted of the sum observations of a community. Given some basic individual freedoms, such as those

86. Times, *Senate Investigators Examining Reports of Faulty Credit Ratings*.

of a current US citizen, there is no functional way to exclude people from consuming the available SCI any more than there is a way to exclude people from speaking with one another. The good therefore, is non-excludable. Additionally, as use of the SCM to obtain information by one user does not prevent another from obtaining the same information, it is non-rivalrous. 'Asking around' about a community member doesn't make subsequent 'asks' by others any less valuable: the information gleaned will be the same.

SCMs therefore were largely public in nature until the advent of the CRA industry. During the industry's development, a market-enhanced SCM superseded the historic, public SCM model. While the enhanced model still wasn't rivalrous, as at its core the information being collected was still non-destructively consumable, it was exclusionary. Both by putting a price on the SCI, and by concentrating high-quality SCI in the hands of a few firms, what had been a very commons-like, pure-public good, developed a pay-to-play character, and transitioned into an excludable club good. Finally, we can see Lloyd's lack of moral restraint in the actions of the CRAs, which though not precisely in keeping with his grazing example[87], well captures the element of tragedy we see associated with securitization.

Given this framing, it seems that in the case of the FCRA, the evolution of what had been a pure public good into an impure public good was central to the eventual securitization of the industry. This evolution occurred naturally due to economic and cultural forces, and functionally resulted in individuals being increasingly excluded from participation in, and most importantly, access to, the newly enhanced SCI. This exclusion exacerbated fears of abuse by those excluded, and produced a lackadaisical, morally-lenient attitude toward information accuracy by the new SCM gate keepers: the CRAs. The aforementioned Times article tellingly provides evidence for both states.[88] The federal investigator who described people as "frightened" succinctly captured the fear of the excluded, while the story of a man who lost his job due to a CRA refusing to correct records falsely indicating he'd had his car repossessed demonstrated significant callousness, if not outright malice, on the part of the CRAs. It was in this climate of growing public concern that the 1967 hearings took place.

However this developing sense of tragedy was not the only influence at work. Outside the relatively specific emerging issue of CRA negligence, there existed in 1960s America

87. Though a commons is rivalrous when used beyond its carrying capacity while the enhanced SCM introduced excludability, both provide opportunities for damaging lacks of moral restraint, result in situations requiring similar responses, and both follow a pure-public toward private trajectory. After last version, this may be misleading..

88. Times, *Senate Investigators Examining Reports of Faulty Credit Ratings*.

a growing fear of dehumanization. During the 1950s, increasing computer use in business had by the 1960s caused punch cards to be common items, largely due to the cost-saving potential of using them for billing purposes. As Steven Lubar writes, unenviably, punch cards became the "interface between the public and the billing system. Metaphorically, they were where the public meshed with the corporate world. They became symbolic of the whole system."[89] The fact that these cards were often marked with the phrase "Do not fold, spindle or mutilate" powerfully suggests how the public felt about the world they symbolized. While folding and spindling are typical office actions, mutilation is glaringly not. Lubar cogently connects the warning's presence on the cards to the broader 1960s zeitgeist which also included the Vietnam War and the Free Speech Movement. In addition to consumer billing activities, both the draft, and various administrative tasks at the University of California at Berkeley (UCB) and other institutions of higher learning were card based, and the destruction, or mutilation of those cards was a powerful symbol of resistance to perceived dehumanization.

In his famous speech given at UCB in 1964, Mario Savio captured this feeling, saying "you've got to put your bodies upon the gears and upon the wheels ... upon the levers, upon all the apparatus, and you've got to make it stop! And you've got to indicate to the people who run it, to the people who own it, that unless you're free, the machine will be prevented from working at all."[90] Reflecting on Savio's speech, Lubar draws particular attention to Savio's use of words like "apparatus" , "gears" and "machine" as likely having more a more literal connotation than being simply suggestive of a "mechanical metaphor for society"[91]: punch card machines. The students had seized on a technology they interacted directly with, and their rhetoric reflected this. It is hard, considering securitization, to ignore this twinning of technological or machine imagery with systems increasingly perceived as opaque and untrustworthy. Likewise, it is hard to ignore Savio's proposed solution to the misguided machinations of the UCB administration machinery being "your bodies" .

Over the period beginning with the conclusion of WWII and ending with the American withdrawal from Vietnam, optimism gave way to skepticism, even cynicism. Given this, it is easy to see the general acceptance of a credit-oriented culture of consumption as an

89. Steven Lubar, ""Do Not Fold, Spindle or Mutilate": A Cultural History of the Punch Card," *Journal of American Culture* 15, no. 4 (1992): 43–55, doi:10.1111/j.1542-734X.1992.1504_43.x, eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1542-734X.1992.1504_43.x, https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1542-734X.1992.1504_43.x.

90. Seth Rosenfeld, *Mario Savio's FBI Odyssey / How the man who challenged 'the machine' got caught in the gears and wheels of J. Edgar Hoover's bureau*, San Franciso Chronicle, October 10, 2004.

91. Lubar, ""Do Not Fold, Spindle or Mutilate": A Cultural History of the Punch Card."

outcome of optimism. Over time however, the honeymoon high waned. Creditors began aggressive debt collection policies like the garnishment of wages without adjudication based in some cases on nothing more than the word of a single CRA.[92] As stories surfaced of people losing their jobs, or having their lives seriously disrupted due to clerical errors on the part of CRAs, and with the 1960s anti-war, anti-establishment rhetoric in full swing, consumers grew increasingly uneasy with the opaque, closed world of the CRAs. From this perspective, the increasingly opaque nature of CRA decision-making, and the grave consequences those decisions could have on individuals without means of recourse, parallels both the UCB administration Savio railed against, and the DoD and its war. Individual Americans were being excluded. As the DoD placed more and more emphasis on its inhuman quantification of success in Vietnam, the body count, unrest and distrust at Lubar's 'system' grew.[93]

It eventually became untenable for elected officials to support the war, and so action was taken; the United States withdrew its forces from Vietnam. Similarly, by the end of the 1960s, it had become so commonly acknowledged that the non-transparent nature of the credit reporting industry was injuring consumers, that action was taken; the FCRA was passed. What began as a market emerging to meet a new demand introduced exclusion in a place it hadn't existed before and users reacted negatively. In response, and amplified by the cultural climate, the most powerful authority available was tasked with investigating and regulating the market. The state assumed some authority over the CRAs in order to enforce Lloyd's moral restraint through the exclusion of what a majority of representatives considered immoral practices. As such, the passage of the FCRA serves to demonstrate essential characteristics of securitization, and further suggests other common qualities of modern security.

One such suggestion has to do with how, as technological change increases in relatively free-market economies, needs arise more quickly, and are in turn met more quickly. Though exclusive, ad-hoc sharing of credit information had been happening since 1803[94], it was not until the credit-loving lifestyle of post-WWII America dramatically increased demand for accurate credit information that the CRA market blossomed. In conjunction with novel information processing techniques (e.g. punch cards and systematizers[95]) the industry grew in a matter of 20 years to a point where it was determined by public opinion to require

92. Times, *Senate Investigators Examining Reports of Faulty Credit Ratings*.

93. Scott Sigmund Gartner and Marissa Edson Myers, "Body counts and" success" in the Vietnam and Korean Wars," *The Journal of Interdisciplinary History* 25, no. 3 (1995): 377–395.

94. Watson, *An abridged version of the Experian: the story so far*.

95. Martin Campbell-Kelly, *Computer: A History of the Information Machine* (Routledge, 2018).

oversight, and it happened largely before the industry was computerized. This would seem to suggest that there may be a relationship between the speed at which something transitions away from a known form, and the speed with which that transition generates alarm. In our terms of securitization, this might suggest that the faster a commons-like tragedy is perceived to be occurring, the faster the calls for a respondent, exclusionary action. We will revisit this in subsequent events, as we move forward chronologically.

The securitization of the FCRA was the result of market forces creating a new, unregulated space, which lead to perceived tragedy due to a lack of moral restraint by some members of the new community. When that perceived tragedy reached a critical mass, authority was invoked to enforce moral restraint. While market forces may have created the CRA industry with their value-added SCI, they were not the only forces at work. The public, the fundamental source of the CRAs' raw materials and whose fate the CRAs increasingly held, were also acted upon by cultural forces. The anti-establishment, anti-war, pro-free speech movements, and an associated fear of dehumanization all acted to amplify the perception of individual tragedy. Securitization clearly does not take place in a vacuum, nor is it necessarily the result of a single tragic incident. Further, though the growth of the CRA industry had already introduced exclusion before tragedy occurred while Lloyd's tragedy of the grazing commons had no exclusion, the tragedy in both situations was the result of a lack of restraint in the absence of regulation. The chosen solution in both cases was the appointment of a regulatory authority.

5

The Morris Worm

5.1 Narrative

Robert Tappan Morris, the son of Bell Labs researcher and National Security Agency (NSA) computer specialist and cryptographer Robert 'Bob' Morris, was born in November of 1965 in rural New Jersey. Bob and his wife Anne were pragmatists, growing their own food when it became expensive, preferring to use hand-me-down appliances and repair them instead of purchasing new ones, and accepting television into the living room after determining their then six year-old daughter to be "mass-culture 'illiterate'" .[96] Young Robert read voraciously, finishing the complete *Lord of the Rings* trilogy in third grade, and distinguished himself in school: a slump in grades correctly attributed to boredom was remedied by having him skip fifth grade entirely. Robert continued to excel academically, and soon became interested in his father's line of work, especially what we might now term 'systems security.' As a teenager, his study of the Unix operating system lead him to uncover a flaw that allowed privileged access to one machine to provide privileged access to any networked machine. After exploring a little, he told the Bell scientists about his discovery and they fixed the vulnerability.

Robert attended Harvard University, where he majored in Computer Science, but spent much more time working on projects of his own, and developing his Unix knowledge than he did on his school work. During his time at Harvard, Robert earned a reputation. Beyond being known as one of the few people that seemed to actually enjoy reading Unix operating manuals, Robert was known as something of a prankster. One April fool's day Robert modified the network login such that it appeared to users that the Harvard network

96. Katie Hafner and John Markoff, *Cyberpunk: outlaws and hackers on the computer frontier, revised* (Simon / Schuster, 1995), 272.

had reverted to an antiquated version of its operating system. On another occasion, after noticing how often people mistyped 'mail' as 'mial', he wrote some code to launch a game when 'mial' was typed, instead of the expected response of 'no such program'.[97]

Jumping ahead to 1988, Bob had moved from Bell labs to direct the NSA's National Computer Security Center, and Robert was just beginning his graduate studies at Cornell University. At Cornell, Robert continued to pour over the Unix manuals and source code, discovering several new bugs. He was particularly excited about a bug in the *ftp* program which allowed arbitrary files to be read or written on a remote machine. At the same time, the notion of viruses was entering the public sphere; the September 26th, 1988, edition of Time was devoted to the idea.[98] In this atmosphere, and given the bug he had found in *ftp*, as well as bugs in *fingerd, rexecd* and *sendmail*, Robert began writing what was to become one of the most famous programs in the history of computing, what would later be termed the 'Morris Worm'. It should be noted, as was pointed out by many experts at the time, that though Robert and his friends referred to his program as a virus, and though it was also commonly referred to as such in the media, it was in fact a worm.[99]

On the evening of November 2nd, Robert finished modifying his program, remotely accessed a machine at the MIT Artificial Intelligence Laboratory, and from it executed his program. Through a combination of poor choices regarding reinfection rates and the presence of bugs, the worm spread much faster than he seems to have anticipated[100][101]. By late that night, Robert was aware he had done something serious, and contacted his closest friends back at Harvard. Robert gave them instructions on how to stop the worm, but these needed to be transmitted using the Internet, which was by this point too bogged down to get the information to the right people.[102] By the morning of the 3rd, the Internet community was reeling. Initially, 6,000 hosts are thought to have been infected, though this number appears to have little validity beyond a wild guess.[103] A later estimate based on a survey of computer centers conducted by a Harvard researcher found that between

97. Hafner and Markoff, *Cyberpunk: outlaws and hackers on the computer frontier, revised*.

98. Susan M Mello, "Administering the Antidote to Computer Viruses: A Comment on United States v. Morris," *Rutgers Computer & Tech. LJ* 19 (1993): 262.

99. Donn Seeley, "A Tour of the Worm," 1989, `http://www.cs.unc.edu/~jeffay/courses/nidsS05/attacks/seely-RTMworm-89.html`.

100. Eugene H Spafford, "The Internet worm program: An analysis," *ACM SIGCOMM Computer Communication Review* 19, no. 1 (1989): 17–57.

101. Ted Eisenberg et al., "The Cornell commission: on Morris and the worm," *Communications of the ACM* 32, no. 6 (1989): 706–709.

102. Hafner and Markoff, *Cyberpunk: outlaws and hackers on the computer frontier, revised*, 304.

103. Paul Graham, "The Submarine," 2005, `http://www.paulgraham.com/submarine.html`.

1,000 and 3,000 computers were likely infected.[104]

Over the next two days, experts across the country worked to decompile and reverse engineer the code, eventually uncovering the vulnerabilities that the program exploited, and releasing patches to address them. The Defense Department was particularly worried that the program contained some kind of destructive capacity - such as file deletion - and the discovery of a timed portion of code sent the reverse-engineers into a frenzy until it was determined that there was in fact no portion of the program that modified files on infected hosts beyond what the program needed to propagate itself.[105]

When the dust settled, the US General Accounting Office, commissioned by Congress to investigate the impact of the event, estimated that the worm caused dollar losses between $ 100,000 and $ 10 million. However the amount of time the report devotes to covering costs is relatively small compared to the amount of time it spends speculating on the implications of the incident: the real impact. As the first Internet-wide security event, it plainly revealed the dangers of the ad-hoc way the network was managed, and the dangers inherent to its decentralized nature. These problems principally manifested themselves in the lack of a central command structure for dealing with network-wide problems, and the related difficulty of distributing critical information like patches.[106] Writing less than a month after the incident, and after having studied the response and the program itself, Eugene Spafford of Purdue University went out of his way to underscore how the decentralized nature of the Internet, and the open nature of both it and Unix aided the spread of the worm while at the same time allowing it to be defeated fairly quickly.[107]

By the morning of November 5th, the New York Times had determined Robert to be the author of the worm, and ran an article titled *Author of Computer 'Virus' Is Son Of N.S.A. Expert on Data Security.* The night before, Robert had travelled home to meet with his parents and pursue legal advice. Within days, Robert had legal representation, but it would be three years before he would be sentenced and lose his appeal. Having been found guilty on one felony count of violating the Computer Fraud and Abuse Act (CFAA), Robert was fined $ 10,000, and sentenced to three years probation and 400 hours of community service.

The case was far from trivial, however, as it was the first jury test of the CFAA which had only been enacted in its then current form in 1986. Resoundingly, the case demonstrated that for a successful CFAA prosecution it was not necessary to show that a defendant

104. Hoy et al., *Computer Security: Virus Highlights Need for Improved Internet Management*.
105. Hafner and Markoff, *Cyberpunk: outlaws and hackers on the computer frontier, revised*, 309.
106. Hoy et al., *Computer Security: Virus Highlights Need for Improved Internet Management*.
107. Spafford, "The Internet worm program: An analysis."

intended to cause damage, or *mens rea*.[108] The case was also widely considered to have brought to light a schism in the Computer Science and Internet communities. It was thought that one camp saw Robert's action - though perhaps somewhat botched - as having been generally positive for the community by driving home the importance of security. Bob Morris, for example, had been writing and giving talks for years trying to draw attention to what was perceived by some as a potentially catastrophic lack of interest in security. Among those who in some way lent their support to Robert during the trial were Ken Thompson, Fred Grampp, Doug McIlroy and Jim Reeds, all of Unix fame.[109]

The supposed alternative camp consisted of people who saw Robert's actions as inherently criminal and dangerous. Some thought that he should serve some jail time, at least in part to dissuade others from similar acts. A false, but widely cited remark typifies this position, and the degree to which the division in the community was blown out of proportion. Purdue's Spafford - who after the worm's release became an ethicist and toured the US lecturing on computer security and ethics - was misrepresented in an Association for Computing Machinery (ACM) article as having said that any technology firm that hired Robert should be boycotted.[110][111] As a member of the Computer Science community, this stood in stark contrast to the much more moderate line being taken by the likes of Thompson. This confusion, abundant differing opinions regarding Robert's criminality or lack thereof, and the general lack of consensus as to what the Computer Science community felt about it underlines the reason that the 'Morris Worm' became so famous. Within days, his worm brought computer security into the mainstream in a way that years of his father's traditional evangelizing had been unable to.

In language which wholly debunks the apocryphal anger Spafford felt toward Robert after the worm incident, Spafford, in a 2008 interview with Network World remarked "I think [Robert] should even be considered for a pardon because since then he's done nothing in his career to take advantage or to gain stature from the incident. He was contrite. . . . He has gone on to have a productive career."[112] Following the worm debacle, Robert went on to co-found Viaweb - which was purchased by Yahoo for $ 49 million and rebranded

108. Mello, "Administering the Antidote to Computer Viruses: A Comment on United States v. Morris," 270.
109. Hafner and Markoff, *Cyberpunk: outlaws and hackers on the computer frontier, revised*, 336.
110. Ibid., 346.
111. Eugene H Spafford, "Three letters on computer security and society," 1991,
112. Carolyn Duffy Marsan, "Where is Robert Morris now?," Network World, 2008, `https://www.networkworld.com/article/2268914/lan-wan/where-is-robert-morris-now-.html`.

'Yahoo! Store' - and Y-Combinator, earn his Ph.D from Harvard and become a tenured professor of Electrical Engineering and Computer Science at MIT.[113]

5.2 Securitization

Before considering the securitizing affect of Morris' worm, it is valuable to consider how it differed from the contemporary event of West German hacker Markus Hess using networks to steal US government secrets. First, while Hess began breaking into machines in 1986, his name was first made public in August of 1989 when he was indicted by West German authorities, nearly a year after Morris' worm. Additionally, though Clifford Stoll (astronomer turned amateur computer-intrusion investigator) first broke the story of his pursuit of Hess in May of 1988, "certain details were necessarily omitted."[114] Stoll's written account of his pursuit, *The Cuckoo's Egg: Inside the World of Computer Espionage*, published in 1989, spent its longest stint on the New York Time's best-seller list in the winter of 1990-91.[115] By contrast, within three days of Morris releasing his worm, his name, along with his father's, and their association with the NSA was featured on the front page of the New York times.[116] Finally, and most convincingly, Morris represents a much larger break from tradition than Hess does. Where Morris was found guilty of a computer crime, Hess was convicted of espionage. Further, where Morris' worm set off an almost immediate, and public debate to do with the merits of limit-seeking behavior, and the open nature of networks and digital resources, Hess for many intents and purposes was just another cold warrior, albeit one who took advantage of that same openness.

This decidedly modern securitization of the developing Internet which Morris ushered into existence, as pragmatic as his upbringing had been, was made possible due in part to a divergence between the spirit of the Internet community, and its technological realities. In exploring the securitizing effect of Morris' worm, this divergence forms the basis for a commons-like tragedy through developing good impurity, and reinforces the dangers of a threat model out of touch with reality. To facilitate this process, we will begin by

113. Kaitlin Quistgaard, "Yahoo Buys Portal-Puzzle Piece," Wired, 1998, `https://www.wired.com/1998/06/yahoo-buys-portal-puzzle-piece/`.
114. Clifford Stoll, "Stalking the wily hacker," *Commun. ACM* 31, no. 5 (1988): 484–497.
115. New York Times, *Paperback Best Sellers*, February 10, 991, `https://timesmachine.nytimes.com/timesmachine/1991/02/10/949391.html`.
116. *Author of Computer 'Virus' is son of NSA expert on data security.*, 1988, A1.

considering the situation from the perspective of a commons and its associated tragedy, before also treating the event in terms of threat modeling and the role exclusion played.

The spirit of the networked-computing community, as it existed from its inception through the late 1980s was that of a pure public good. Hafner & Markoff capture this state effectively in contrast with today, writing "In the late 1970s and early 1980s, security had yet to become a serious issue on college campuses." [117] Today, it is college campuses where high-end cyber security is most prominent in many people's lives, if only because, as institutions that accept federal money and store data ranging from health to financial information, they are required to adhere to data-protection standards far higher than most non-governmental organizations. This open spirit, and lack of security at the very institutions which had already had such a big impact on the development of the Internet, appears to share much in common with the pure-public ideal.

It is somewhat difficult to perfectly map the notion of rivalry and excludability onto a technology like the Internet, however a slightly loosened notion fits easily. Unlike the classic non-excludability of clean air, there is an outright exclusivity mechanism for the Internet due to its inherent reliance on human-built infrastructure: the vast majority of Internet users pay for their service. So though the Internet may in spirit be purely public, in practice it is not. Like clean air however (at least when restricted to personal consumption, not major polluters, which is the classical context) the design of the Internet encapsulates the idea of non-rivalry, and indeed much effort has gone into ensuring that many users can simultaneously access a system through, for instance, time-sharing protocols and multi-user operating systems. Further, it is generally considered an essential quality of an Internet-capable service that it be non-rivalrous, which can serve only to underline the fundamental nature of non-rivalry on the Internet. This mentality is today reflected in technologies like load balancers, content delivery networks and the ubiquitous use of caching. The Internet is therefore, by design, best characterized as an impure public good, or a club good; excludable but non-rivalrous. Tellingly, denial of service (DoS) attacks and their distributed variants (DDoS), which continue to be among the most common types of cyber attacks launched, attack the functional non-rivalry of a target. A target is considered compromised only if users begin to experience rivalry.

Given this characterization of the Internet as functionally a club good, we may pursue the same analysis, and the Morris incident is indeed suggestive of the same basic two step process we saw in the securitization of the CRA industry. Morris' 1988 worm served

117. Hafner, K., & Markoff, J. (1995). Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York: Simon & Schuster. p.67

to draw attention to the issue that, in fact, the Internet was extremely rivalrous in the presence of software like his worm. The nascent Internet was revealed in an even less pure-public light than it had been previously. Further, Morris' trial hinged on whether or not his intention had been to cause damage, and a large camp sustained that he had simply been exploring. As most classically public goods are susceptible to some degree of rivalry due to intentional abuse (clean air may be poisoned) this feature of Morris' worm is critical. Not only did it demonstrate that a skilled miscreant could cause serious damage, but that mistakes made during the course of well-intentioned use could also introduce extreme rivalry. The fact that Morris' trial hinged on *mens rea,* the factor which distinguished those two potential threats, served to draw attention to both. If not only malicious, but well-intentioned actions could also result in rivalry contrary to the principles of the Internet, the purity of the Internet good was degraded.

Perhaps the most direct, literal effect of the Morris worm was the establishment of a Defense Advanced Research Projects Agency (DARPA) funded Computer Emergency Response Team (CERT) at Carnegie Mellon University (CMU).[118] The worm had, among other things, resoundingly demonstrated the flaws of having no centralized response infrastructure. Containment, debugging, note sharing and other response activities all utilized the Internet, which if damaged as a whole, crippled the channels which could be used to facilitate its repair. The CERT was to, in part, provide alternative channels for such activity, and establish a formal protocol for responding to threats to the Internet. Such threats, made mainstream by the Morris incident, have come to characterize the Internet: a heavily securitized Internet. In this way, the CMU CERT quite clearly fits our paradigm of the establishment of an authority in response to apparent impurities in the public nature of a good. Further, as Morris' prosecution was the first under the newly passed Computer Fraud and Abuse act, it represented a proof-of-concept: the potential for abuse was real, and the value of authorities taking responsibility for the Internet was useful and valid. The securitization of the Internet was cemented in its most formal form yet.

Though the worm may have represented a proof-of-concept with regard to the specific technologies involved, in terms of the damage suffered as a result of a divergence between doctrine and reality, it played out an age-old pattern. While there were members of the extended computer science community pushing for increased attention to security during

118. Michael Gervais, "Cyber attacks and the laws of war," *Journal of Law & Cyber Warfare* 1, no. 1 (2012): 8–98.

the 1980s - prominent among whom were Willis Ware, Robert Courtney Jr., and Robert Morris' father, Bob - they seemed to be gaining little to no traction. Concerted with that lack of traction, there seems to have also been a general preference for convenience over security. Susan Landau in *Listening In*, cites the prevalence of passwordless 'guest' accounts as exemplifying this attitude, and indeed such features were abused by Morris to facilitate his worm's ability to propagate. The story of the limited success of the Orange Book, and of businesses like IBM building security products which emphasized usability over security further reinforce the decade's stance on security.

In addition to an apparent preference for convenience, system administrators in the 1980s perceived their opponents to be minimally dangerous. According to Landau they "believed their adversaries were teenagers or university students. They weren't expecting intrusions by proficient hackers and therefore did not develop protections to stop them."[119] This would seem to suggest a disconnect between the technology itself and the practices of the people involved in overseeing that technology. Throughout the 1970s and 1980s, various industries were transformed by computerization, as for instance was the credit reporting industry. As we have already seen, small errors in CRA data could wreak serious havoc in people's lives even before computerization. In an industry heavily computerized in the 1970s, the capability for damaging hacks clearly existed in the 1980s, a realization not at all captured by system administrators dismissing their potential adversaries as children. By the end of the 1980s however, that posture had been forced into closer alignment with the technological realities of the era.

Joseph Coates foreshadowed this realignment in 1983 when he wrote of the potential benefits of a cataclysmic computer security incident:

"The computer industry is so complacent, its buyers and users so beguiled by the equipment, and regulators so enchanted by the relative calm as computers spread across all of society, that the industry needs its equivalent of Hiroshima to wake up and alert the nation to the enormous risks latent in the way we organize our computer affairs."[120]

Contemporaries of Coates, writing in the same early-80s period were also clearly aware of the extant danger posed by computer insecurity. In the same volume of the *Computer Security Journal* that featured Coate's article, Donn B. Parker, author of the 1967 book *Computer Crime* wrote, somewhat optimistically as it would turn out, that the "start of the exponential growth of computer crime cases in 1967 may be indicative of an awakening

119. Landau, *Listening In: Cybersecurity in an Insecure Age*, 47.
120. Joseph F. Coates, "The Future of Data Security," *COMP. SECURITY J.* 2, no. 1 (1983).

of public interest in the subject. . . .”[121] Insiders like Coates and Parker were keenly aware of what was going on, and for more than a decade had been collecting data on security incidents. However, as both attest to, the majority of those incidents were related to abuses or mistakes internal to organizations, a fact which had dual oppressive effects on the public's awareness of computer security issues. First, companies naturally feared to admit they had experienced an incident for the generally bad press it generated, a fear compounded by the likelihood of the perpetrator having been an employee or contractor.[122] Additionally, they feared spreading knowledge of the means of attack, as would be required if they were to take a case to court. Both forces grew in power the larger the incident was, as the bigger the theft the bigger the headlines, and the greater the potential damage of copycat attacks. Compelling evidence for this state of affairs can be found in Robert Courtney Jr.'s description of the relationship between a security incident's dollar cost, and the likelihood that the injured party would prosecute.

“If you plot the probability of prosecution when you know all you need to do to make a case, against the magnitude of the loss you'll find about 85% of the cases involving less than 1,000 dollars, there's an attempt to prosecute. At a 250,000 dollars it's 50-50. At a 1,000,000 dollars it's four percent, and [at] 4,000,000 dollars it's one percent!”[123]

While computer experts may have had the computer expertise, they lacked the audience to make a large, culture-affecting impact. *WarGames* ended up picking up the slack. Unusual for movies that depict hacking, the *WarGames* plot was one which featured highly realistic and effective hacking. Yet even after the blockbuster opening of *WarGames* managed to get the attention of Ronald Reagan, little fundamental action was taken. As we've seen, industry continued to oppose a security-first posture, and as Landau pointed out, passwordless guest accounts were still common at the time Morris launched his worm. Despite widespread appreciation among computer experts for the dangers of lax security, and popular fiction like *WarGames*, the state of the early Internet was not one which focused on security. As Aspray & Ceruzzi write “the popular press at the [time of Morris] was obsessed with Microsoft and its chair Bill Gates, and ignored news of networking activities.”[124]

The 1980s computer security doctrine simply didn't reflect the reality of the situation. Administrators' basic threat model of bored teenagers had been unfortunately reinforced

121. Donn B. Parker, “How much computer abuse is there?,” *COMP. SECURITY J.* 2, no. 1 (1983).
122. Robert H. Courtney Jr, “Untitled” (11th Annual Computer Security Applications Conference, December 1995).
123. Ibid.
124. Paul E Ceruzzi and William Aspray, *The Internet and American Business* (MIT Press, 2008), 25.

by incidents involving teens, including the famous 414 gang[125], and by *WarGames*, which despite drawing attention to some very real issues of network security, was still essentially the story of a bored teen. In this light, it is easy to appreciate what Coates saw as the intractable state of the 1980s computer security threat model, and his sentiment that the field would benefit from a Hiroshima-like event.

What Coates evokes with references to the atomic bombing of 1945 is a watershed moment. However it was not a single event that caused the Japanese to surrender. It serves us here simply to note that the Japanese strategy at the time of Hiroshima and Nagasaki was already a defensive one, indicating that the bombings did not take place in a vacuum nor singularly determine the outcome of the War, though they no doubt had an outsized effect. In this way, Morris' worm fits well the watershed, yet nonsingular moment, the benefits of which Coates was suggesting. As the second half of the 20th century was one marked by nuclear threat modeling, so the post-Morris era has been one marked by broadening, increasingly hacker-aware threat modeling.

In the developing perception that the Internet's open nature was being made less pure we see a tragedy take shape. When Coates wrote of people's "relative calm as computers spread across all of society"[126], he provides insight into a 1980s version of the same dramatic, natural rise of a technology or service we saw in the explosive growth of the 1950s and 1960s CRA industry. In both instances, as their existence became more and more widespread, they tragically introduced malaise in areas which like a Samaritan commons below capacity, had previously been healthy.

Tragedy in the case of Morris came in many forms. A series of events in the 1980s leading up to the release of his Worm had warned again and again of the dangers of insecure networks. However these warnings, largely due to having not engaged the self-interest of the business community, had tragically failed to induce substantive behavioral change. Whether viewed as malicious or accidental, the worm was itself destructive in that it both brought the work of thousands of researchers to a standstill and in the real-dollar losses it caused. Each of these tragic elements stem from the Internet's developing impurity and a public appreciation thereof. Over the course of the 1980s, the early Internet's commons-like zeitgeist of openness was tragically unveiled as dangerous. The result was again exclusion.

125. Bruce Middleton, *A history of cyber security attacks: 1980 to present* (Auerbach Publications, 2017), 11.

126. Coates, "The Future of Data Security."

In some cases exclusion was implemented through higher authorities, as in DARPA funding the establishment of a national CERT at CMU. In other cases it was those same administrators whose threat model had just been so jarringly updated who took it upon themselves to, at the very least, improve their exclusionary capabilities. Evidence for this can be found in a greater attention paid to the quality of passwords in the post-Morris world. At the Dutch *Centrum Wiskunde & Informatica* (CWI) for example, one of their lead computer-center administrators wrote an article just a year after Morris' worm which reflects both exclusion and an at least partially updated threat model.[127] Daniel Karrenberg, after noting how their center had recently become available from all over the world, explored the possibility of segmenting, or literally excluding, certain portions of their computing resources in an externally-inaccessible intranet. He also evangelized for high-quality passwords, following what's hard not to interpret as an oblique reference to Morris: "more sophisticated intruders are known to try out a lot of passwords in order to get access." Finally, Karrenberg also addressed some of the human issues related to those improved exclusionary tactics. He, for instance, reminded users not to share their passwords, despite the practice's apparent time-savings.

Karrenberg's article represents an early step in the updating of the outmoded 1980s security posture. Morris' worm, and the pursuit and eventual exposure of Markus Hess by Clifford Stoll eviscerated the out-of-date model of teenagers and bored students.[128] Morris, a bored student himself, demonstrated that despite their position, students, and indeed anyone with access to an Internet connection could cause enormous damage. Further, not only could such an individual cause great damage intentionally, but bugs in honest, well-intentioned software could also have serious consequences. A bored master's student had taken advantage of convenience oriented features, fundamentally challenging both the established threat model, and the ethos of usability over security.

Barely two years later, when the full extent of Hess' activities came to light in 1990[129], it became clear that teenagers weren't the only bad actors against whom defenses needed to be organized; professional hackers also existed. Though sites connected via the Internet had contained potentially sensitive information since their first interface message processor (IMP), outside of explicitly government run facilities (ie. those connected via MILNET), there seems to have been little to no sensitivity to what would now seem an obvious need to protect such information. MILNET was separated from ARPANET in 1983,

127. Daniel Karrenberg, "Password Security," *CST Bulletin*, 1990,
128. Hafner and Markoff, *Cyberpunk: outlaws and hackers on the computer frontier, revised*, 272.
129. *Hackers found guilty of selling computer codes*, 1990,

suggesting that there existed concerns over security in the military, yet the persistence of the 'teenagers and convenience' ethos of the 1980s indicates that, in general, the practices of system administrators and those tasked with maintaining Internet infrastructure were not keeping pace with the changing technology.

By highlighting the inadequacies of the 1980s threat model, and doing it with an eye-popping price tag, Morris' worm and the subsequent court battle securitized the industry in a way previously difficult to imagine. The entire community was forced to take sides, which regardless of side chosen caused the issue itself - the inherent insecurity of the Internet - to take center stage. After Morris, convenience was re-evaluated as being less important relative to security; a reformulation that necessarily kept more closely to the technology. Like the popping of a market bubble indicates a widespread acceptance of there being a disconnect between value and price (ie. a correction), the Morris worm represented a correction in the the valuation of security. Practices were updated to better handle the state of technology.

6

CWI

6.1 Narrative

In 1946, the Foundation Mathematical Science (MC) was founded with the stated purpose of "foster[ing] the systematic pursuit of pure and applied mathematics in the Netherlands".[130] Among the MC's methods for achieving this are the promotion of research with industry applications, consulting activities, the provisioning of computing facilities, and the running of lectures and conferences. The foundation is funded by the Netherlands Organization for the Advancement of Pure Research (ZWO), now named the Netherlands Agency for Scientific Research (NWO). In 1983, MC was renamed to Centre for Mathematics and Computer Science (*Centrum Wiskunde & Informatica*, CWI) to express the increasing importance of computer science.

The MC had from its inception been home to a computer department, which through the dedication of the first ARRA, the Automatische Relais Rekenmachine Amsterdam, in the summer of 1952 precipitated The Netherlands into the computer age. Also in 1952, hiring Edsger Dijkstra for programming the ARRA, Adriaan van Wijngaarden, head of the Computation Department, ingested a Dutch tradition of programming and software development. The MC exerted a major influence on the programming language ALGOL 60. ALGOL 68 may even be considered Van Wijngaarden's brainchild.[131]

The renaming and reorganization of 1983 was in part designed to more accurately reflect the specific fields of study the institute was engaged in, and would appear to also reflect the growing appreciation of Computer Science not as a branch of Mathematics, but as an independent field In a similar move, once the MC was unable to keep up with

130. CWI, *Annual Report '83*, Centrum voor Wiskunde en Informatica.
131. CWI, *Annual Report '87*, Centrum voor Wiskunde en Informatica, Section titled "In Memoriam A. van Wijngaarden".

the computing needs of Amsterdam's universities, a role it had traditionally played, the universities and the MC jointly founded the academic computing center SARA in 1971. Taken together, one begins to get a sense of a field universally acknowledged as valuable but uncertain of auspice, burgeoning in sometimes unexpected directions.

The late 1960s and 1970s saw the development and free distribution of AT&T's UNIX operating system around the world. According to Davies, this was one of, if not *the* watershed moment in the computer community embracing an open ethos in favor of the proprietary orientation which had hitherto held sway.[132] Evidence for the popularity of this transition can be found in the rapid formation of UNIX community organizations that sprang up throughout the 1970s which in the US included the now famous USENIX. In Europe the CWI was the first spot for UNIX to land and it spread from there. By the end of the 1970s, similar community growth was taking place in Europe in the form of many "UNIX User Groups" or UUGs. Many countries developed their own UUG; in Dutch the national UUG was referred to as NLUUG, while the European-wide group, formed in 1981, was called EUUG. Critical to this community-based expansion was the development of the "UNIX to UNIX copy protocol", or UUCP, and its use as a store-and-forward networking protocol. UUCP was originally designed to reduce the cost of distributing increasingly large softwares, most notably UNIX, but its wider networking capabilities quickly became apparent.[133] In order to communicate and share data, or network, two machines running UUCP on UNIX simply needed to establish a telephone connection between them. Originally included in AT& T's 1977 release of their UNIX distribution, UUCP was almost immediately employed as a way to distribute information within organizations and institutions, especially email, and after the official announcement of UUCPnet at USENIX in 1980, its use grew rapidly.[134] Additionally, the development of newsgroup software, and its free distribution in 1980 drew yet more people to the technology.[135]

Early European UUGs, which included the national groups of the Netherlands and United Kingdom, became increasingly interested in UUCP, and developed an interest in starting their own network based upon it. While an almost purely ad-hoc design ruled in the monolithic United States, Europe with its more complicated regulatory environment,

132. Howard Davies and Beatrice Bressan, *A history of international research networking: The people who made it happen* (John Wiley & Sons, 2010), 79.
133. Ibid.
134. Julie K Petersen, *The telecommunications illustrated dictionary* (CRC press, 2002), 939.
135. Davies and Bressan, *A history of international research networking: The people who made it happen*, 79.

consisting as it did of multiple national entities with their own laws, protected industries and patchwork agreements, posed a serious networking challenge. The greater EUUG community eventually settled on the establishment of a single, national UUCP host node capable of establishing international connections, each responsible for accepting their own intra-national communications. The result was EUnet. In its earliest stages, EUnet's operation was not segmented from the Dutch national network, which were both centered at the soon-to-be CWI. Along with the Netherlands, Sweden, the UK and Denmark joined to form the first multinational European UUCP network, which was eventually able to connect its US counterpart through the CWI in Amsterdam.[136] Piet Beertema, who became the "central technical manager" of EUnet at CWI recalls that the EUnet's central machine was called 'mcvax', indicating its location at the MC, and the type of machine it was.[137] The node would come to be world famous.

Over the course of the 1980s EUnet rapidly expanded to include nodes in nearly all western European countries, links to places as far afield as Japan and Australia, and even connections in some Warsaw Pact countries.[138] The 1980s also saw Daniel Karrenberg oversee the development and deployment of the Internet Protocol (IP) throughout the EUnet, and the establishment of the first "open" IP connection between the US machine 'seismo' at the University of Maryland's Seismological Institute, and mcvax at CWI.[139][140] Incidentally, the establishment of the transatlantic IP connection on November 17th, 1988, which connected EUnet to NSFnet, came just two week after Morris' worm had wreaked havoc on US computing centers.[141] Beertema refers to it as the "dreaded Morris worm" , and notes that the establishment of a second transatlantic link soon after the first was at least in part designed to act as the backup channel, the value of which the worm had so violently demonstrated.[142]

Given this situation in the 1980s, the CWI was clearly central to the development of networking, not only in the Netherlands, but in all of Europe. Given the foundation's background which well predates the networking activities of the 1970s and 1980s, considering the changes the MC and CWI underwent as networks emerged as a mainstay in computing may prove insightful. Naively, the simple fact that the CWI was distinguished

136. Ibid.
137. Piet Beertema, "Piet Beertema's web site," 2019, `https://godfatherof.nl/`.
138. Davies and Bressan, *A history of international research networking: The people who made it happen*, 83-84.
139. Beertema, "Piet Beertema's web site."
140. Davies and Bressan, *A history of international research networking: The people who made it happen*.
141. Ibid., 84.
142. Beertema, "Piet Beertema's web site."

from the MC supports the excitement surrounding computers and networks. Through the CWI's end-of-year reports, we begin to develop a much clearer picture of exactly how computing was affected by not only technological developments, but as echoed by Beertema, human developments like the release of Morris' worm and the computing culture of the time.

In the first report issued by the newly distinguished CWI, the index includes a section titled "Computer Science", followed by "Supporting Services", and "Computer Equipment" .[143] The Computer Science section, in keeping with the other "Science" sections[144] depicts the activities of the group's members, and focuses on the projects being pursued by each. The Supporting Services section describes its purpose as "support[ing] the scientific departments", as well as handling similar needs by outside firms and interests.[145] Though it's mentioned that the CWI is "the management of EUNET, the European Wide Area Network of UNIX, for which CWI is the backbone centre", the overall tone of the report suggests that the department exists in an almost entirely supportive role.[146] The last section, Computer Equipment, lists the available hardware. Such a clear delineation of roles, particularly between 'Computer Science' and 'Supporting Services', was to undergo rapid change in the context of the 1980s networking fervor.

The first, 1983 CWI end-of-year report's Supporting Services chapter contains three sections, "Contracts and Support Division" , "Library" and "Publication Department" , and fails to take up a single, full page. In 1986, there appeared a "Computer Systems and Telematics Sector" section, abbreviated CST, which cites the increasing usage of personal computers and the ever expanding EUnet and USENET as chief challenges. In 1987, CST is described as having "both a service/support and a research role" , which included "networking support on behalf of the EUUG and NLUUG" and "research on Euromath." [147][148] The next year, CST was upgraded to quasi-full department status. In the introduction to the 1988 report, the CWI's then-director P.C. Baayen wrote:

"Computer Systems and Telematics was originally tasked with supporting operating systems and networks. The appointment of a departmental head in 1988 marked expansion to a full research-oriented component of CWI's computer science departments."[149]

143. CWI, *Annual Report '83*.
144. A "Science" section corresponds roughly with a fully fledged research department within the CWI.
145. CWI, *Annual Report '83*.
146. Ibid.
147. Euromath was a European Commission sponsored project designed to foster inter-national operability in mathematics research
148. CWI, *Annual Report '87*.
149. CWI, *Annual Report '88*, Centrum voor Wiskunde en Informatica.

The chosen head was Dick Bulterman, and the listed members of the department included the aforementioned Daniel Karrenberg and Piet Beertema. Under Bulterman, the CST continued to take on a stronger research orientation. It also began to publish bulletins of its own. The first Bulletin's explanation of why it exists beautifully captures the CST's evolving role, and the rapid development of computing at the time:

"Recently the number of computer users at CWI has grown considerably. The times when the people of the 'Computer Lab' met all users regularly are over. Because many new users do (and can) not read important announcements on the net news, there is a need for a new medium through which everyone can be reached. Hence this Bulletin."[150]

The author of the statement, Lambert Meertens, in lamenting the end of the 'everyone meeting regularly' era, at once captures the rapid transformation of the field taking place, as well as the need to update security protocols in the face of distributed access. The times when physical security effectively equated with computer security were over. At the same time, Meertens' conflation of users' ability and will to abide by the rules perfectly parallels the sense of computer security Coates, Courtney, Parker and their colleagues were developing: the vast majority of computer security incidents hitherto had been the result of sometimes malicious, sometimes accidental computer use by a company's or institution's own members. To a large extent, they argued, the external threat was a straw man, at least by measure of the relative money being spent on external-penetration defenses compared to user training and internal auditing.[151][152][153] While Morris' worm certainly amplified fears of the external threat, his worm's exploitation of poor passwords - particularly as it facilitated lateral movement - in fact underscores their point. Today it has become clear that both are important, as both have been demonstrated to be potentially very dangerous.

In the 1988 CST bulletin, a brief section on backups written by Bulterman updates this insider/outsider divide. Remarking on a recent, unfortunate loss of data, he wrote "While it is unclear if this was the work of a small (but resourceful) group of international terrorists, or simply 'one of those things that happen', these two occurrences do provide a useful background for the restatement of the CST backup policy." Regardless of agent or malicious intent, adherence to the rules is important. Though his tone seems jovial, at the time of writing Italy's Red Brigades and the French Action Directe terrorist groups

150. Lambert Meertens, "Introduction," *CST Bulletin*, 1983,
151. Courtney Jr, "Untitled."
152. Parker, "How much computer abuse is there?"
153. Coates, "The Future of Data Security."

had both recently attacked computing centers.[154] With hindsight Bulterman's statement appears particularly premonitory. However his comments, along with those of Meertens in the CST Bulletins, and the rapidly changing role of the CST within the CWI are highly suggestive of the degree to which the CST's internal culture was both a product and a reflection of the changing times.

6.2 Securitization

The story of the CST's existence during the transition from mainframe-based computing to a network and pc-based model, and its relatively unique organization, make it a particularly interesting lens through which to consider securitization. Karrenberg recalls that it was a "very challenging and interesting environment full of good ideas" where, like Ware before them, people from different backgrounds and interests would "mingle and talk to each other", both formally and "in the hallway on the blackboard."[155] Speaking to the CWI's agility in providing for research needs, Bulterman described the environment as "light-weight", and indicated that, enviably, they had access to "tons of money." He also noted that not having a student body to support, with their tendency for the "unorthodox", made administration easier.[156] This efficient, well financed space that fostered innovation and protected the creative direction of its members underwent what can be seen as a very slow securitizing process.

The tragedy element of the tragedy of the commons phenomenon is realized when a lack of regulation, or the old mode, somehow becomes a problem. At the CWI, those old ways were characterized by security enshrined in physical spaces. Meertens' lament, and Bulterman's contention that the reason the CST Bulletin existed was because "things [didn't] work anymore by word of mouth", both support a growing sense of the inevitable end of an era.[157] Yet while they are both in terms of people, they also capture the initial stages of networked computing which was becoming increasingly unconstrained by geographic location. For instance, the ability to 'dial in' to computing resources from off site, dramatically increased the functional attack surface of such centers.

Mr. Bulterman's experience working at a highly-secure Air Force base captures the physical security that was rapidly dissipating over networks. He described having a Lieu-

154. Michael Alexander, "High-tech boom opens security gaps," *Computerworld* 24, no. 14 (1990): 118–119.
155. Daniel Karrenberg, *Interview*, June 26, 2019.
156. Dick Bulterman, *Interview*, July 4, 2019.
157. Ibid.

tenant minder whose job was to accompany him to the bathroom and ring a bell as they went, as "a sign to all the people that they had to cover any classified information because I ... was a threat - because I was physically [there]." He further recalled that rats chewing on cables was the main security problem during early computing endeavors at the CWI.[158] In the absence of facility-traversing technology, computer security and facilities security were functionally synonymous. Today, physical security is no less important that it was before the rise of networks, however many more concerns have been added to what was a very traditional, fairly contained attack surface. It is perhaps somewhat melodramatic to call this tragedy, but from our abstract framing of the tragedy of the commons, it fits well. The old mode of security was no longer sufficient, and new, necessarily more distributed forms of exclusion were required. Another way to view this transition is in terms of trust. Where in the everyone-knows-everyone era it was important to trust the people you were around, it became increasingly important to instead trust the machine. If due to the increasing size of the user community you could no longer be sure if someone was vetted or not, it became necessary to trust that their individual access to resources was secure.

A compounding effect of the increasingly networked nature of computing is suggested by Bulterman's assertion that the "real [security] milestone was Windows ... because it was so widespread, and it was a common platform."[159] The widespread use of Windows created a value-adding incentive for attacks against it, as the ratio of required exploits to payout was greater than that of less widely used platforms. In this way, homogeneity attracts attention, and relative to physical computing facilities, networking protocols are highly homogeneous. One implication of homogeneity as risk, is the potential for diversity as security. A recent investigation into low-level implementations of diversification for the purposes of security described the process: "diversification breaks the 'monoculturalism' and introduces 'multiculturalism' in the software deployment process."[160] The parallels between this, calls for diversity of various kinds by likes of Tabriz and the call for the diversification of research directions within computer security that resulted from the 2008 WSS, are difficult to ignore.

Additionally, the emancipation of security from physical spaces at the CST during the late 1980s closely parallels the ever-changing computer threat model of the times. In the US, where open networking had been already growing for nearly a decade, the result of

158. Ibid.

159. Ibid.

160. Shohreh Hosseinzadeh et al., "Diversification and obfuscation techniques for software security: A systematic literature review," *Information and Software Technology*, 2018,

this emancipation was threat-modeling that identified bored students and teenagers as the primary source of problems: a feeling WarGames epitomized. Bulterman echoes this sentiment for Europe. When describing security problems during his time at the CST, he remarked "back then it was much more of a student thing. For a while it migrated out to kind of the high school kids."[161] Predating the kids however, and despite close interaction between computer enthusiasts on both sides of the Atlantic (all three of our European interviewees spent time working or teaching or both in the US) there existed a threat in Europe which didn't exist in the US. Though terrorist activity was present in both places, in Europe, terrorist groups like the Red Brigades had physically attacked computing facilities.[162] There is little evidence to support this having had much effect on the CST group, however it drives home the fact that the physical model was not incorrect, it was simply not destined to last.

It follows that the securitization ultimately undergone by the CST at CWI, while similar to what was happening around the world, was to a degree uniquely European. It was a product partially of the enthusiasm that innovators like Karrenberg, who once acquired and illegally (at the time) connected a dialer so as to better participate in emergent networking activities, had for networking technology. At the CST, it was also a result of an interest in exploring new areas, both out of sheer curiosity and for the purposes of producing publishable research. Karrenberg described the then-scientific director of the CWI, Cor Baayen, as trying to foster such a pragmatic culture. "He didn't want to have some people just in a room running a network, but he wanted to have people in a room running a network and [have them] talk about it."[163] Bulterman also positions Baayen, and the then-administrative director of the CWI Jan Nuis, as critical to the protection of the pursuit of open standards within the CWI at a time when the PTTs were powerful agents for the use of proprietary protocols. "[Nuis and Baayen] were always very supportive and thought actually it was kind of interesting", and even "backed up that we would do it our way".[164] This was particularly important in the context of European networking achievements which faced stiffer resistance from the interconnected web of PTT relationships than their counterparts in the US did.

In the story of the CST, we see perhaps more cleanly than in previous cases, a slow realization that the old era was waning, and with it a host of traditions. From our perspective here, the most interesting of those traditions was that of physical security

161. Bulterman, *Interview.*
162. Courtney Jr, "Untitled."
163. Karrenberg, *Interview.*
164. Bulterman, *Interview.*

as equivalent to computer security. As computing, which had emerged in the form of monolithic mainframes, dissipated over networks into PCs and into homes, the attack surface of computing resources expanded dramatically. It became increasingly important to secure systems at the granularity of the machine or individual system, and not at the person, since the person was no longer necessarily available. As the emancipation of security from facilities control continued, the CWI eventually encountered problems with people parking in their lots, attempting to use their wireless networks. As we will see in the next chapter, this increasingly anonymous access quickly came to provide a vector for rampant lacks of moral restraint.

Finally, the CST story is also highly suggestive of the effect that the perceived speed of tragedy has on the resultant securitizing action. At the CST, around the time in question, there was relatively little abuse, and as such any gaps between threat-model and reality were not highlighted as they were in other cases. The CWI therefore seems to have not reacted dramatically to the end of an era, but rather to have taken in stride the emerging need to implement security measures on machines, and via system administrators. For a variety of reasons, of which the relatively low-value market of the academic research stored at the CWI cannot be ignored, the CST avoided a Coatesian Hiroshima.

7

The Metro

7.1 Michael van Eeden, Hacker Turned Admin

By the time Robert Morris was being tried for releasing his famous worm, the Internet had already experienced its first what we might now call 'killer application', electronic mail.[165] Synonymous with the technology at the time was MCI (originally for Microwave Communications Inc), which since its inception as a private network link provider had by 1988 grown into one of the single largest commercial email providers in the world. As Alfred Glossbrenner wrote in the 1990 version of his digital Reader's Digest, "People may have accounts on different systems, but everybody is on MCI."[166] That same year, Tim Berners-Lee and his colleagues at CERN were deploying the first version of what would soon join email as the Internet's other killer application, the World Wide Web.[167] Taken together, these events usefully depict the state of networked affairs at the beginning of the 1990s.

Morris brought the intrigue of computing into the mainstream and generated a spirited public debate over the norms developing with regard to the nascent Internet. That same public, it turned out, found email "so compelling that people were prepared to purchase an entire computer system in order to use [it]" .[168] Combined with the rise of the personal computer and the networked, distributed model of computing popularized in the 1970s, computer outsiders were increasingly adopting the technology. As Janet Abbate synthesized these forces, growing public interest in the domain was linked to the increasingly

165. Ceruzzi and Aspray, *The Internet and American Business*, 105.

166. Alfred Glossbrenner and Alfred. Going online Glossbrenner, *The complete handbook of personal computer communications* (St. Martin's Press, 1990).

167. Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor* (DIANE Publishing Company, 2001), 30.

168. Ceruzzi and Aspray, *The Internet and American Business*, 105.

attractive graphics of personal computer systems, while the web combined those visuals with the power of networks.[169] The web provided "an easy on-ramp to the information superhighway"[170] beginning to engage the self-interest of more and more consumers. Since the first successful HTTP communications in December of 1990, the web has grown to the point where it's often confused with the Internet itself.[171]

A final appeal to Abbate completes the staging for this chapter's instance of securitization, the story of hacker turned administrator Michael van Eeden. Speaking to the commons-like properties of the Internet we have touched upon in the previous sections Abbate writes:

"The Internet community's decentralized authority, its inclusive process for developing technical standards, and its tradition of user activism encouraged new groups to participate in expanding and improving the network, and the openness of the system invited users to create new applications (of which the World Wide Web would be the most dramatic example)."[172]

Mr. van Eeden's story is that of a prototypical hacker. Dutch by birth, Mr. van Eeden recalled his first hack being a joint effort undertaken by himself and friends at a Museum in the Hague that in the mid 1970s had just opened a computing exhibit. The youths managed to find a copy of the display computer's programming manual, and from it learned how to ring the systems' physical bells. Eventually they discovered that they could send these commands remotely, and began setting off bells in Utrecht, where the Museum terminals' mainframe was located, much to the chagrin of the Utrecht administrators.[173] In high school, Mr. van Eeden's enthusiasm for computing gave him a natural leg up on his classmates, and even his instructors. Eventually his teachers simply let him teach his classmates programming principles.[174]

After graduating from high school, Mr. van Eeden faced an ugly choice. Though he had been making money working at software companies, he generally found computing to be boring. He described his options as "either University, or this whole IBM world, with suits."[175] Mr. van Eeden chose art school, though he kept working in the computing field in various capacities. Eventually, having grown bored with art school, an opportunity arose

169. Janet Abbate, *Inventing the internet* (MIT press, 2000), 212.
170. Ceruzzi and Aspray, *The Internet and American Business*, 38.
171. Berners-Lee and Fischetti, *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*.
172. Ceruzzi and Aspray, *The Internet and American Business*, 182.
173. Eeden, *Interview*.
174. Ibid.
175. Ibid.

that allowed him to continue exploring. At one of his side jobs he encountered language-learning software written by a French company which he found to be of exceptionally poor quality. He wrote to the company, explaining that he had quite a few ideas on how to improve their software, and included a fictional "external expertise report" which he offered the company for 10,000 dollars. They invited him to visit and offered him a job on the spot, which he accepted. The move was likely made easier by his having recently fallen in love with a French woman. At his new firm, Mr. van Eeden convinced his boss that the company should "get into sound" which resulted in the 21 year old jet setting between Europe and the west coast of the US as he developed business relationships with American firms - particularly Sound Master. He recalls thinking at the time, "this is the life!"[176]

After bouncing around for a while, including a stint at an American company based in Colorado where he encountered MCI mail, Mr. van Eeden moved back to the Netherlands in 1993. Such a transatlantic existence perfectly situated him to appreciate the killer-nature of the email app, of which he reminisced that "It was really amazing you know, [sic] communicat[ing] with someone electronically overseas." Back in the Netherlands, Mr. van Eeden found an opportunity to explore the middle ground he'd bemoaned the lack of between suits and academia. It came in the form of an Amsterdam civic initiative to more closely integrate the city's population with their representatives called *The Digital City (De Digitale Stad* or DDS*)*. When Mr. van Eeden learned of the project in the newspaper, it immediately piqued his interest and he set about trying to get involved as any hacker would, by hacking. As it turned out, the DDS was being administered by the Dutch telecom service provider Hacktic (now XS4All), that just so happened to have a program that rewarded successful penetrations of their system (if they were told about it) with an apple pie. Mr. van Eeden "hacked through the night" , and eventually discovered that the email program they provided, called *Elm*, would drop to prompt if the user-tunable default mail editor was set to a shell interpreter and editing was requested. He was in.

Having claimed his apple pie, and gotten involved in the administration of the DDS, Mr. van Eeden joined the ranks of those who didn't fit either end of his academia-to-suit spectrum. In his words, his colleagues only common feature was that "they didn't look like anyone else... who looked the same. They were a little bit punk." He continues that they "were not really interested in rules and laws" , citing by way of example that "they would experiment with drugs."[177] Despite this, "they really did have a hacker ethic. They

176. Ibid.

177. Though Mr. van Eeden was aware of this, he didn't participate ibid.

were not at all criminal." From this, and Mr. van Eeden's operationalization of hacking as being done "out of curiosity", there emerges a strong sense of the centrality of *mens rea* to cyber activity, just as we saw highlighted by Morris' trial. There is a clear tension between what Mr. van Eeden sees as the ethically upstanding motivations of "out of curiosity" and "seeing if it can be done" , and the potential for such approaches to lead to real, tangible damage.[178]

Eventually, the DDS would become web-based, but before that happened, Mr. van Eeden had built an Object-Oriented Multi-User Dungeon (OO MUD, or MOO) which gave DDS users the ability create their own content and post it for others to see. Modeled after Amsterdam's subway service, he called his MOO *the Metro*. Almost immediately, users began to seek its limits. Mr. van Eeden recalled that one early limit pusher began to fill his space with Nazi content, forcing the hacker-minded van Eeden to step into an authoritative role. After his colleagues responded to his requests for advice with "it's your Metro, you decide" , he sought a metaphor upon which to base his custodianship. He likened his role to that of a manager at a youth center or playground. Such a place is designed to be free in the sense that the children can do whatever they want, but there is still an authority to make sure that, as Mr. van Eeden put it, "it wouldn't get out of hand."[179] In the end he recalls finally settling on some basic rules which banned, among other things, "sexism" and "racism" , and winding up as a kind of "dictator" .[180] The limit pusher had become the limit setter.

There is perhaps no better evidence for the script flip undergone by van Eeden than his reaction to being asked whether or not the Nazi propagandist's actions were that of a hacker in the limit-pushing sense. He responded "No, yea, maybe you could call it hacking."[181] Nazism is near canonical evil, yet the damage potential of the Metro user was much more difficult to gauge than that of Morris' worm. The GAO, in some cases, was able to rely on quantitative measures like a computer center's down time and the average cost of staffing to establish damage in dollars.[182] While few would argue that a bored student's apolitical, nonviolent hijinx is as evil as what resulted from Nazism, the dividing line, as with *mens rea*, is fuzzy. In his reaction we see him grappling with this problem, going through machinations not unlike those undergone by the computer science community during Morris' trial. Indeed rights of free speech, which encourage the same

178. Eeden, *Interview*.
179. Ibid.
180. Ibid.
181. Ibid.
182. Hoy et al., *Computer Security: Virus Highlights Need for Improved Internet Management*, 17.

boundary-pushing behavior espoused by hackers, stop short of fully embracing "seeing if it can be done" . Regardless of motivation, it is unethical to shout "fire" in a crowded theatre.[183]

7.2 Securitization

Mr. van Eeden's Metro manifested Abbate's vision of the Internet as an inclusive, activist-friendly place where openness invited creation. It was a place that allowed for the free expression of thought and provided anonymity at previously difficult to imagine levels by virtue of its digital, networked nature. In many ways, the Metro was a utopian commons. There was functionally very little exclusion beyond technological requirements for access and limitations due to, for instance, the total number of users then-versions of Unix supported. Mr. van Eeden recalls that "sometimes we just had to [take down user-generated content], because it would generate so much traffic."[184] Noting that this was almost always porn related, he continued "[we took it down] not because we're against porn, but just because we couldn't handle it." The pragmatic, anti-exclusion, anti-rivalry ethos this reflects on the part of the DDS admins is perhaps the best evidence for the Metro's utopian qualities. Functionally, there were limits imposed upon the system, but they were contrary to the overall design.

The Nazi propagandist whose posts eventually lead to the introduction of rules caused the Metro to experience rivalry, but a form unlike porn directories generating too much traffic. Not only did people find the content offensive, but its uncontested presence within a system operating under the auspices of the state endangered the entire project. The Netherlands, it should be noted, banned Mein Kampf after WWII, and would understandably not be thrilled to be associated with something that could be called Nazi sympathetic.[185] In an instance of textbook rivalry, one user's apparent lack of moral-restraint

183. The free-speech counterbalancing notion of "shouting fire in a crowded theatre" stems from a justice's preamble to the 1919 US Supreme Court decision Schenck v. United States which established a "clear and present danger" requirement for limiting free speech. The precedent, which at the time was used to convict anti-war activists under the Espionage Act, was reformulated in 1969 in Brandenburg v. Ohio (which ruled in favor of the Klu Klux Klan's right to publish hate speech) to the much stricter need for speech to be "directed to inciting or producing imminent lawless action and [being] likely to incite or produce such action." (Trevor Timm, "It's time to stop using the "fire in a crowded theater" quote," *Atlantic* 2 [2012])

184. Eeden, *Interview*.

185. Bruno Waterfield, "Ban Koran like Mein Kampf, says Dutch MP," *The Telegraph*, 2007, `https://www.telegraph.co.uk/news/worldnews/1559877/Ban-Koran-like-Mein-Kampf-says-Dutch-MP.html`.

endangered the ability of all other users to continue to use the system whatsoever, inherently limiting the value they could derive from the Metro, let alone the intrinsically offensive nature of the Nazi material. Mr. van Eeden and his fellow hacker administrators, though not having anticipated such a situation, identified it as potentially problematic for these reasons, and responded to protect their system. Though leary of turning into the authorities they collectively found antagonistic, a pragmatic need to keep their system alive overrode other concerns. The Metro underwent securitization, just as the CRA industry and greater Internet before it, as a result of what the admins perceived as an impurity growing so rapidly in their digital commons that it threatened its very existence. Begrudgingly, they reacted by banning practices they deemed dangerous to their greater project.

Compared to the securitization of the CRA industry, Mr. van Eeden adopting authority over his Metro is a microcosm, and indeed we see the same paradigm we saw in both the passage of the FCRA and in the story of Morris' worm. That first, most macro event, involved an entire nation's public perception of a tragedy, and resulted in the nation's highest agreed upon force for coercion being tasked with establishing rules. While technology, like punch cards, certainly played a role in the securitization represented by the FCRA, the entire story is one with a technological character, not one that exists within a technological setting. In moving forward chronologically, we have also moved into the technology, the events having become further inscribed within computers and networks. Establishing when the first SCM arose is perhaps best done at a millenia granularity, while establishing when the Internet emerged, given assumptions we are perfectly capable of evidencing empirically, is possible at a day or week granularity. The area which underwent securitization was ancient in the case of the FCRA, and less than a century old in Morris' case. Considering Mr. van Eeden's Metro in this way suggests it to be a further technological circumscription. Where Morris' worm affected the securitization of a specific technology, the Metro was one of many spaces enabled by that specific technology.

This narrowing of scope sheds light not only on the fundamental components of securitization, but also speaks to how powerfully the ever-increasing speed of technological development may affect securitization. Partially by virtue of the length of time SCMs have existed, there were many extant forms, practices and associated organs in the late 1960s when the industry underwent the securitization of the FCRA. There was, for instance, little uncertainty as to what entity should take up the enactment and enforcement of regulation. Morris' worm hinted at the benefits of such established structures, at least in so far as the lack thereof exacerbated his worm's damage. However there was still little

question that the eventually established CERT would be a joint Federal and academic venture, because that is whom tradition identified as the proper authorities. In contrast, Mr. van Eeden was in essentially uncharted waters.

It was not just the admin's reaction to the Nazi content which lacked historical basis. In describing his reaction to the first copyright infringement takedown notices he received regarding material on the Metro, Mr. van Eeden remarked "Well we didn't know what to do! We didn't know if we were responsible, or if the user was responsible." On the general security posture of the DDS operators, he remarked that "there was no formal policy like you would have now" , concluding "I think the whole security model was completely based on this one hacker ethic that we all had."[186] In the absence of precedent, they fell back on their hacker ethic, and the securitization of the Metro took a decidedly hacker flavor. There would be no sweeping rules, save those required to safeguard the existence of the greater system, and there continued to be an appreciation for the merit of limit-seeking behavior - to a loose, pragmatically defined point.

Corroboration of this newness of form can be found in the unpleasant story of the securitization of a MOO contemporary with the Metro called LambdaMOO. In 1993, Julian Dibbell wrote an article for The Village Voice titled *A Rape in Cyberspace* which tells the story of the users of LambdaMOO working through the aftermath of one of their members abusing the environment's features to digitally commit sexually explicit acts as other users' characters without their consent. In text rife with allusions to "wizard, master programmers" , Dibbell describes the LambdaMOO characters in anthropomorphic language suggestive of a time when computing was still considered magical.[187] Most painful perhaps, is that looking back on the event, it is hard not to find it almost quaint in contrast with what is commonly acknowledged as occurring on the Internet now. It simply would not be a story today, but in 1993 it was a brand new phenomenon. Further, the members of LambdaMOO went to great pains to justify their understandable desire to censure the perpetrator in terms of their personal-freedom oriented ideological positions. As Dibbell described it, "a pro-death penalty platform is not an especially comfortable one for an anarchist to sit on."[188]

Another way to frame Mr. van Eeden's pioneering experience is with the concepts of threat models and attack surfaces. In terms of threat models, one simply didn't exist

186. Eeden, *Interview*.
187. Julian Dibbell, "A rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society," *Ann. Surv. Am. L.*, 1994, 471.
188. Ibid.

for the new space they had created. Older threat models, like those suggested by the Ware report, focused on outsiders. *WarGames* was the story of an outsider in more ways than one; the 414 Gang was remotely breaking *into* computing centers; Morris' worm had spread out of his control *into* systems across the Internet. Mr. van Eeden suggested the ubiquity of this orientation around the time he was running his Metro. When asked if, during his tenure in the jet set, he'd generally encountered security, he responded "this was all offline, of course at these companies we had networks but it wasn't connected to anything." This suggests that his concept of security is one closely related to an outsider-oriented model. An internal network wasn't a security issue unless connected to the wider world, and such a model is not one which immediately lends itself to the internal nature of the Nazi propagandist threat. Given the danger we have seen resulting from threat models out of sync with reality, Mr. van Eeden's sense of security in terms of external threats might have been costly. However it would seem that hacker pragmatism acted as a counterbalancing force against the inertia of the times.

It follows from the wild-west nature of the Metro's development that its attack surface would be constantly expanded as new threats were discovered. Tellingly, after having assumed some authority in defense of the Metro, Mr. van Eeden recalls receiving death threats.[189] Clearly, the Metro's attack surface included Mr. van Eeden. At once, both the attackable surface of the Metro was increased, and the threat model loosely employed by its admins expanded. Ever the pragmatist, Mr. van Eeden tempered his recollection of receiving death threats at around the same time the Nazi propagandist was helping define the limits of the Metro, describing the propagandist as not trying "to be an asshole, but because he wanted to know what can you do. What's possible. So I didn't really mind."[190] Certainly, Mr. van Eeden did mind receiving threats of violence against his person, but his condemnation of the perpetrators seemed tinged with the same conflicted sympathy for the hacker ethic he himself espoused.

Despite being in the uncharted waters of Internet-enabled spaces never-before securitized, the securitization of Mr. van Eeden's Metro followed the same paradigm we have seen in the other events, core to which is the notion of exclusion. Minimally, the fact that the limit-pushing van Eeden himself established limits is powerful testimony for the necessity of exclusion as a component of protecting something's future. Further, the story of the Metro is highly suggestive of the influence that an individual's or group's background, tradition and ideological orientation have on the way exclusion is enacted. The

189. Eeden, *Interview*.
190. Ibid.

loose exclusion introduced into the Metro after tragedy was perceived contrasts starkly with the legalist, technocratic measures imposed by the FCRA. Finally, the pragmatic securitization of the Metro in relation to Morris' worm illuminates just how difficult it is to establish whether or not a particular limit-seeking activity is "positive" , and establishing *mens rea*. It would seem that the position of authorities called upon to enact exclusion on the authoritarian to hacker spectrum greatly affects the perception of tragedy, and therefor securitization. A consideration of *mens rea*, regardless of tragedy, serves to establish a community-normalized notion of what is acceptable and what is not. Once done, such norms serve as a tradition which may be appealed to during subsequent security incidents, as was the case with the FCRA. Assuming that the inertia generated within a community through such determinations acts upon future security considerations, early events, like the traditionless Metro limit-pushing may have an outsized impact on the long term security posture, and character of a system.

8

2007 Estonian Cyber Attacks

8.1 2007 Estonian Incident

On the night of April 27, 2007, a statue was removed from a busy intersection in the middle of the Estonian capital of Tallinn, and relocated to a military cemetary a short distance away. Beneath the statue were the graves of a number of Red Army soldiers who perished in World War II. The incident touched off several days of riots in Tallinn, and sparked what later became known as the 'Cyber War I'.[191] Though for all intents and purposes, the relocation of the statue was a classically political move, several factors specific to Estonia and the era made it unique. We will first consider the classical elements, and then unique features, and finally interpret it in terms of securitization.

In 1944, as the Nazis retreated before the Red Army, Estonia briefly enjoyed sovereignty, at least in name, between approximately the 18th and the 22nd of September, during that period an Estonian flag flew over their seat of government, replacing a Nazi flag, and preceding a Soviet flag. In multiple separate actions, the Red Army defeated Estonian forces, and proceeded to occupy the country. A widespread resistance movement began, but was largely crushed by 1950, at least in part due to mass deportations of suspected sympathizers and family members to Soviet Gulags.[192]

It was during this period in 1947 that the bronze statue central to the 2007 incident was erected in the center of Tallinn to commemorate the three year anniversary of the 'liberation' of Estonia from the Nazis. It was called the "Unknown Soldier" , and sat atop

191. Kertu Ruus, *Cyber War I: Estonia Attacked from Russia*, 2008, `https://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia`.

192. Olaf Mertelsmann and Aigi Rahi-Tamm, "Cleansing and compromise. The Estonian SSR in 1944-1945," *Cahiers du monde russe. Russie-Empire russe-Union soviétique et États indépendants* 49, nos. 49/2-3 (2008): 319–340.

a small Red Army grave site. Estonia would remain an occupied territory until the fall of the Soviet Union some 50 years later, and during that time the area's ethnically Russian population grew significantly: constituting roughly a quarter of the population by 2007. Given its background, it is no wonder that a statue which ethnic Russians consider a monument to the sacrifice of the Red Army, and which some Estonians call the "Unknown Rapist" would lend itself to political tension.[193]

We will not delve into the particulars of the political machinations that lead to the decision to move the statue in 2007, as this background information is intended only to reinforce the issue as classically political. However, regardless of political bent, the statue had become a focal point for tension between ethnically-Estonian and ethnically-Russian Estonians by early 2007, and for various reasons, the Estonian government decided it was time to move it. On the 26th of April they erected a tent over it, and established a police cordon. Over the next two days, as the authorities worked to move the statue, protests grew into riots, eventually leading to one death, and widespread looting.[194] As the riots subsided, a two phase cyber campaign was beginning. Russian 'hacktivists' targeted the Estonian government's web presence for defacement and denial of service, egged on by Russian-language media.[195]

The commencement of cyber attacks on a nation's core infrastructure is the first of the unique factors at play in the Estonian incident. After a few days of these amateurish attacks, Estonian authorities noticed a substantial uptick in the traffic bombarding their government and big-business services. They had come under attack from much more sophisticated, highly distributed sources. This enhanced attack managed to disable parliament's email, and caused disruption in several large Estonian banks and media outlets.[196] With the benefit of a decade's worth of hindsight, it would seem that the incident was not particularly devastating in terms of systems disrupted. However, like Morris' worm, it served to shake up the status quo, and represented a major paradigm shift in the understanding of the balance of power in cyberspace.

In order to explore this shift, it is first important to appreciate the second unique component of the incident: the Estonian state's aggressive adoption of e-governance and

193. Ruus, *Cyber War I: Estonia Attacked from Russia.*

194. Steven Lee Myers, "Russia Rebukes Estonia for Moving Soviet Statue," *New York Times*, April 27, 2007, accessed March 1, 2019, `https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html`.

195. Ibid.

196. Mark Lander and John Markoff, "In Estonia, what may be the first war in cyberspace.," *New York Times*, May 28, 2007,

high technology. In a description touted by Estonia's own 'e-estonia' promotional site[197], Wired last year referred to Estonia as "the most advanced digital society in the world" .[198] The facts back this up. After it gained independence in the wake of the fall of the Soviet Union, Estonia sought to distinguish itself from its Baltic neighbors through digitalization, and by 1997 had begun to roll out 'e' systems.[199] By 2000 the majority of Government services were available via the web, and most tax filings were done electronically. Famously, Estonia completed a national election via the Internet in 2005.[200][201]

Though the 2007 incident was classically political, due to the 'e' nature of Estonia, several features of the event stand out as unique, if not transformational. First, like Morris' worm before it, the realization of the potential danger of a nation-wide cyber event, and the clear links to the Russian influences caused the predominant threat model of "lone hackers and script kiddies" to be reexamined.[202] Where Morris' worm and the unmasking of Markus Hess had demonstrated the potential damage of lone-wolf attacks and the potential sophistication of so called "bored students", the attack on Estonia demonstrated the potentially enormous destructive power of a well-financed, state-assisted cyber assault. No longer were lone wolves the baddest actors around.

Secondly, as asserted by Otis in his analysis of the 2007 cyber attack on Estonia, the event exhibited all the features of a 'people's war', the requirements for which, building on previous Chinese work[203], he enumerates as variety in agents, external motivation of agents, and the existence of state support. There is substantial evidence to support the cyber assault on Estonia as a people's war. Indeed, through its obstinate resistance to abide by post Soviet legal cooperation treaties with Estonian law enforcement in relation to the incident, Russia implicated itself to a significant degree.[204] However, despite a widespread belief that the Kremlin had at least some hand in orchestrating the incident, or at least fanned the flames, little action has been taken. Certainly no action in keeping with the 'war' rhetoric so often associated with the incident. As Otis notes succinctly,

197. E-Estonia, "We have built a digital society and so can you," `https://e-estonia.com/`.
198. Ben Hammersley, "Concerned about Brexit? Why not become an e-resident of Estonia," *Wired*, March 27, 2017,
199. Ibid.
200. Lander and Markoff, "In Estonia, what may be the first war in cyberspace."
201. E-Estonia, "We have built a digital society and so can you."
202. Rain Ottis, "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective," in *Proceedings of the 7th European Conference on Information Warfare* (2008), 163.
203. Chris Wu, "An Overview of the Research and Development of Information Warfare in China," in *Cyberwar, Netwar and the Revolution in Military Affairs* (Springer, 2006), 173–195.
204. Ottis, "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective."

"The beauty of people's war is that it provides near perfect deniability for the government or any other entity that is behind the attacks" .[205]

This plausible deniability, and the Estonian government's decision to treat the event as a criminal act rather than terrorism, or more serious still, an act of war, is at the heart of the third outcome we may observe.[206] Estonia is a NATO member, and thus, under the mutual defense conditions of NATO's Article 5, should the cyber assault have been deemed an act of war, all NATO members would be required to respond. The only Article 5 invocation in the history of NATO was after the September 11, 2001 attacks on the United States which resulted in a broadly-collaborative action in Afghanistan. Though there seems to have been little real consideration of invoking Article 5 in 2007, the shield of plausible deniability in its context was widely appreciated.[207][208] Considering NATO, and similarly binding treaties in the context of cyber conflict, the 'after Estonia' stage of modern international conflict is one that takes full advantage of this plausible deniability, and to a large extent divorces cyber activities from traditional, kinetic terms and language.

In the wake of the cyber attack, several measure were taken. They included setting up the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), which runs *Locked Shields*, one of the most advanced cyber-conflict exercises today, and has famously published two versions of an internationally compiled discussion on law and norms in cyber conflict called the *Tallinn Manual*.[209] In the US, cyber issues, which had no place on the Department of Defense's list of top threats until 2008, soared to number one by 2012.[210] Snowden's revelations in 2013 included information on a 2009 Chinese hack of Lockheed Martin in which they stole huge troves of data to do with the development of the state-of-the-art F-35 jet fighter. The Chinese J-31 fighter, unveiled in 2012 bore a striking resemblance to the F-35.[211][212] At around the same time, in 2010 the public learned of Stuxnet, often considered the first major state-developed cyber weapon.[213]

205. Ottis, "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective."
206. Eneken Tikk, Kadri Kaska, and Liis Vihul, *International cyber incidents: Legal considerations* (Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010).
207. Ibid.
208. Ottis, "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective."
209. Michael Schmitt, "Tallinn manual 2.0 on the international law of cyber operations: What it is and isn't," *Just Security*, 2017,
210. Landau, *Listening In: Cybersecurity in an Insecure Age*, 45.
211. Ibid.
212. David Alexander, "Theft of F-35 Design Data Is Helping US Adversaries—Pentagon," *Reuters, June* 19 (2013).
213. Landau, *Listening In: Cybersecurity in an Insecure Age*, 57.

In the context of these developments, the 2007 Estonian incident would seem to have been a watershed moment in the escalation of cyber activities, marking the public emergence of the nation-state onto the cyber scene. In doing so, nation states may have tipped their hands. For instance, the Tallinn Manuals represent a direct response to the incredibly difficult problem of applying kinetic-oriented legal frameworks to the cyber landscape which Russia utilized to maintain plausible deniability during the attacks on Estonia. This time period, therefore, represents an escalation in the securitization of cyberspace.

It is quite difficult to know with any accuracy what was known by, or going on inside governmental structures prior to the public revelations and events beginning with these attacks. However if we consider public knowledge, they represent the emergence of a new threat, the identification of a new theatre with its own specific, untested set of rules, and a scramble to develop new security aparati sufficient to exercise some control over these new threats. The new threat was the nation-state. The new theater was a previously undefined intersection between international relations and the Internet, and while the jury is still very much out on the outcomes of attempts to establish control over this area, we may with some validity consider modern trends in its context.

Let us consider the development of hypersonic missiles. A hypersonic missile is one which approaches its target at many times the speed of sound; a speed which, in combination with its potential to follow an erratic flight path toward its target renders most extant missile defense systems useless. They may carry either a nuclear or conventional payload, and given the global reach that at least the US currently possesses, would allow Washington to - with only minimal preparation - strike any location in the world within minutes. Hypersonic missile technology is currently a very hot area of research, with the US, China and Russia having all devoted significant defense spending to their development.[214] The most recent US defense budget included 2.6 billion for hypersonic research.[215] Most poignantly, from our perspective here, there is no equal defensive technology, which has lead strategic thinkers to the necessity of states having a 'deterrent' stockpile of their own hypersonic missiles.

It's not hard to see this development of offensive capability, which is by no means a new paradigm, as running parallel to the emergence of the nation-state and the inherent 'grey-space' of international cyber action. In the absence of an overarching authority, and

214. Louis A Del Monte, *Nanoweapons: A Growing Threat to Humanity* (U of Nebraska Press, 2017).

215. Lara Seligman, "Pentagon Eyes Windfall as Trump Seeks $750 Billion Defense Budget," *Foreign Policy*, March 10, 2019, `https://foreignpolicy.com/2019/03/10/pentagon-eyes-windfall-as-trump-seeks-750-billion-defense-budget-military/`.

in the presence of potentially adversarial others, the prisoner's dilemma of how to deal with uncertainty has resulted in a cyber arms race. However, as the Estonian case demonstrated, this parallel is uniquely cyber. For instance, unlike the most recent conventional arms races - most notably nuclear - we have already witnessed a large number of nation states launch cyber attacks against other nation states. Given the similar, yet unique quality of this cyber arms race, the securitization of the theater will naturally follow a similar, but uniquely cyber track; a track characterized by widespread pushing of limits. Where the Cuban missile crisis developed into an almost purely human affair as a result of developments in offensive, kinetic technology, the 2016 US election meddling was one where the actual weapons - hacking, exploitation of big data, 'platform abuse'[216] - took center stage. The 2016 election meddling also serves to demonstrate the continued skew toward offense in the cyber theater, as Russia seems to still be quite successfully benefiting from the lack of an adequate defense against the plausible deniability of a cyber people's war.

8.2 Securitization

It remains to consider the Estonian incident from the perspective of our core concepts. From the preceding, relatively unstructured analysis of the securitization that resulted from the 2007 Estonian incident, we see an instance of securitization which appears parallel to the paradigm present in the previous cases. First, the utopia-heavy rhetoric that has often been associated with Estonia's digital governance supports the idea that, at least to some degree, the space Estonia continues to build possesses commons-like aspirations. Second, throughout the event and its aftermath we see instances of exclusion manifested, from the tragic, exclusionary denial of service produced by the attacks, to Estonian responses that included both literal exclusion and political actions that appeared designed to reinforce feelings of otherness toward their attacker. Finally, the emergence of the nation-state has to a degree defined the last decade of cybersecurity thought - especially the post-2016 election era. Usefully, however, there are features of the Estonian situation which differ markedly from our previous events, providing the opportunity to better understand the general phenomenon through contrast. The most prominent of these features is the historic enmity between Estonia and Russia, and the fact that, as a nation-state, Estonia lacks a ready-made authority from which to request protection.

216. Making use of the fairly loose, commerce-oriented rules on platforms like Facebook.

The aforementioned e-Estonia promotional website provides a tailor-made entry point to considering both the commons-building nature of the Estonian digital governance project, as well as their existential, eastern threat. The site features a synopsis of a 2016 Guardian article from which they have quoted "[Estonia] 'rapidly transformed from Soviet state to digital utopia'" to use as the page's title.[217] Similar references to digital utopia building abound, and in utopianism lies the same tragic vulnerability present in the commons, in no small part due to the assumptions necessarily implicit in such an idealized project. The Utopia imagined by Thomas Moore's 1516 book from which we derive the term featured slavery.[218] Despite critiques suggesting that Moore's slavery was intended to be at least *more* egalitarian than the then-English practice of executing petty thieves - used as it was largely as a punishment for breaking Utopia's laws - Moore's was an era of slavery, and the institution found its way, largely unchallenged, into his Utopia[219]. It is not difficult to see the history of the United States and its 13th constitutional amendment as both literally, and abstractly following the same pattern. Likewise, Estonia's self-affirmed utopian digital-governance ambitions necessarily carries the weight of tradition. In the Estonian case, those traditions clearly included a fraught relationship with Russia, and a threat model that didn't provide for either a nation-state actor, or the related people's war effort.

Fundamentally then, the Estonian experience in 2007 was one which tragically demonstrated a divergence of reality from expectation. Their threat model, though seemingly well informed with regard to Russia, didn't anticipate the emergence of the nation-state. However Estonia can hardly be faulted for having not predicted the next major cyber-security trend, and their response to the sudden, tragic realization of their model's inadequacy is one that seems to have beneficially drawn on traditions of securitization. Most explicitly, they implemented exclusion in several different ways, and managed to achieve a relatively high-level of exclusion with regard to Russia despite not having a supranational authority to turn to.

During the second phase of the incident, when the Estonian authorities noticed that a large portion of the malicious connections originated outside of Estonia, they disabled

217. E-Estonia, "The Guardian: Estonia "rapidly transformed from a Soviet state to digital utopia"," *E-Estonia*, September 2016, `https://e-estonia.com/the-guardian-estonia-rapidly-transformed-from-a-soviet-state-to-digital-utopia/`.

218. Moore Thomas, *Utopia, 1516*, 1965.

219. Shlomo Avineri, "War and Slavery in More's Utopia," *International Review of Social History* 7, no. 2 (1962): 260–290.

many of the connections which allowed Estonia to communicate with the rest of the Internet.[220] This first act of exclusion proved effective in the short term, preserving banking and civil services for the people living in Estonia. The next year, in 2008, NATO founded the CCDCOE in Tallinn. As an organization developed specifically to check Soviet expansion, and which post-Soviet Russia still sees as a direct threat, closer cooperation with NATO effectively distanced Estonia from Russia.[221][222] Despite NATO's supranational existence, the people's war nature of cyber actions, among other political concerns effectively prevented NATO from assuming the securitizing role the US federal government had played when the FRCA was passed, or that Mr. van Eeden played as benevolent dictator. NATO could not act directly. A reaffirmation of vows, backed by real, tangible action on the part of both NATO and Estonia effectively filled the void, albeit not in the exact same form we have seen previously. While no monolithic entity was tasked with enforcing rules, the aggrieved parties agreed to cooperate more closely. Lacking an authority to turn to, the commons grazers resorted to collectivism to improve the commons' ability to withstand unpreventable instances of abandoned moral-restraint.

The final component of the Estonian narrative which makes it so compelling can be seen in how it played out two major, relatively recent developments in cyber security. First, as we have discussed, the emergence of the nation-state as most-dangerous threat actor has unequivocally demonstrated that cyber threats have exceeded international legal structures. The fact that the Tallinn Manuals, despite being called manuals, are chiefly "commentaires" underscores the problem of territory-based laws and political structures bringing their traditions to an inherently global Internet.[223] Second, the tragedy inherent in the utopianism of Estonia's digital-governance project was in the collective realization that a state's national processes and infrastructures were not only vulnerable to cyber attack, but that agents existed who were willing to attack them. This loss of innocence captures the escalating stakes in cyber security. Where Morris' worm instigated the securitization of a relatively new technology, and Mr. van Eeden was forced to securitize a brand new, Internet-enabled space, the 2007 attack on Estonia catalyzed the cyber-securitization of the age-old institution of statehood. The past decade has seen this escalation continue,

220. Patrick Kingsley, "How tiny Estonia stepped out of USSR's shadow to become an internet titan," *The Guardian*, May 15, 2012,

221. Victor Davis Hanson, "Office Hours: VIctor Davis Hanson on NATO," PolicyEd, 2018, `https://www.policyed.org/intellections/nato-21st-century-ensuring-liberal-democracy-europe/video-0`.

222. BBC News, *Russia security paper designates Nato as threat*, December 31, 2015, `https://www.bbc.com/news/world-europe-35208636`.

223. Schmitt, "Tallinn manual 2.0 on the international law of cyber operations: What it is and isn't."

from the State infrastructure of Estonia, to the democratic infrastructure of the 2016 US election meddling.

On top of these nebulous cyber advances is the disparity between offense and defense and the ever-increasing pace of technological development. If time-to-market negatively incentivizes security during the development of a digital technology, the short-termism that so widely pervades our commercial sectors suggests little cause for optimism.[224][225] The cyber arms race compounds this problem, as prioritizing offensive capability over defense will likely result in a less secure cyber environment overall. However Estonia's response suggests possible recourse. Faced with an unprecedented technical challenge wearing the trappings of historical Russian enmity, the Estonians combined a unique technical defense, and a wholly traditional political solution. In this way, the Estonian event, which ushered in improved era in NATO cyber-preparedness and lead to extensive investigations like those reflected in the Tallinn Manuals, possesses many of the characteristics of Coates' digital Hiroshima. While Estonia certainly suffered, it was not wholly in vain.

224. Joseph E Stiglitz, *Rewriting the rules of the American economy: An agenda for growth and shared prosperity* (WW Norton & Company, 2015).

225. Barbara Vieira, "Is software security improving?," *ABN AMRO*, January 24, 2019,

9

2016 US Election Meddling

9.1 Narrative

On December 23rd, 2015, nearly a quarter-million Ukrainians unexpectedly lost power.[226] In the aftermath of what is thought to be the first wide-spread attack on power infrastructure, US investigators determined that the same BlackEnergy malware that was involved in the Ukrainain disruption was present in "numerous industrial control systems (ICSs) environments" in the US.[227] It appeared to US cyber officials that the "sophisticated malware campaign" responsible for the software's presence had been running since 2011.[228] David J. Weinstein, who worked at the US Cyber Command from 2010 to 2013 and was quoted in a recent NY Times article on developments in offensive US cyber activities, likened the 2015 Ukranian event to crossing the Rubicon.[229][230] In invoking the solidification of Caesar's power and accompanying death of the republic, Weinstein manages to at once suggest the seminal nature of an attack on power-infrastructure, and the difficulty inherent in identifying any single event as a beginning. The prosecution of a large-scale cyber campaign with potentially lethal capability, fatalistically supports the former suggestion.

226. David E. Sanger, "Utilities Cautioned About Potential for a Cyberattack," *New York Times*, February 29, 2016, https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html.

227. Cybersecurity and Infrastructure Security Agency, "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)," 2014, https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B.

228. Ibid.

229. David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *New York Times*, May 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

230. News Staff, "Dave Weinstein, Former New Jersey CTO, Heads to Private Cybersecurity Firm," Government Technology, 2018, https://www.govtech.com/workforce/Dave-Weinstein-Former-New-Jersey-CTO-Heads-to-Private-Cybersecurity-Firm.html.

Yet while the Rubicon crossing has been immortalized, Marius' military reforms, Sulla's demonstrably effective use of force for political advantage and the concentration of power in the first triumvirate are also often seen as important components in the Roman transition toward empire. As such, though the 2015 Russian attack on the Ukrainian power grid was certainly an escalation in cyber conflict and in its own right represented a disturbing revision of cyber norms, it was to a large extent driven by the inertia of tradition, one long established in the kinetic world, but also fairly well established in the cyber world. The 2007 Russian attack on Estonia, and the 2008 Russian attack on Georgia, for instance, both targeted infrastructure: governance and communications respectively.[231] In the Georgian case, cyber operations were supported by ground troops, as was Russia's annexation of the Crimea in 2014 and its subsequent eastern Ukrainian operations.[232]

That 2014 Crimean action also saw Russia deploy malware in an attempt to generally discredit election results.[233] This vector for foreign interference in internal matters of state was subsequently brought to the forefront of public awareness during the 2016 Russian meddling in the US presidential election. Just as the Russian actions against Estonia and Georgia reflect this dialectic of the inertia of tradition interacting with the new, so too did the 2016 Russian election meddling reflect both a Rubicon crossing and a slow, inertial march. That march, according to the recently released *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, referred to hereafter as the Mueller report, began in 2014, which corresponds with other, early cyber election meddling like that seen in the Ukraine.[234]

The Mueller report, commissioned by the US Deputy Attorney General (AG) Rod Rosenstein on the 17th of May, 2017, was made public (with redactions) on April 18th of this year. Rosenstein appointed Robert Mueller as special counsel, and tasked him with investigating Russian meddling in the 2016 presidential election, and "any links and/or coordination between the Russian government and people associated with Republican Trump's campaign."[235] Mueller, a former FBI director, spent the next two years running a leakless office and delivered his report to AG William Barr on March 22nd, 2019.[236] The

231. Landau, *Listening In: Cybersecurity in an Insecure Age*, 55.
232. Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Rand Corporation, 2017).
233. Scott J Shackelford et al., "Making Democracy Harder to Hack," *U. Mich. JL Reform* 50 (2016): 629.
234. Robert S Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 2019,
235. Grant McCool and Jonathan Oatis, "Timeline: Big moments in Mueller investigation of Russian meddling in 2016 U.S. election.," *Reuters*, March 8, 2019,
236. Ibid.

only two criminal cases against Russian entities related to the meddling, *US v. Internet Research Agency et al.* and *US v. Netysho, et al.,* stem directly from the two-pronged Russian interference strategy laid out in the report. One prong, related to the Internet Research Agency (IRA), had been performing operations in the US since 2014, while the other, which the Mueller report identified as a "hacking and dumping operation" , began in 2016.[237]

On June 14th, 2014, four IRA employees applied for US visas, "claiming to be four friends who met at a party."[238] Two got in, and reportedly spent some amount of time gathering intelligence; the redacted Mueller report doesn't indicate when they left the US. Despite getting a couple of agents over the border, the IRA - commonly referred to as a "troll farm" - performed mostly cyber activities that could be accomplished remotely. These included the "purchase of political advertisements on social media in the names of US persons" , and the "staging of political rallies inside the US."[239] The operations were funded primarily by Yevgeniy Prigozhin, a Russian oligarch with ties to Putin. Prigozhin, who is known as "the chef" , and who once served George W. Bush caviar, runs both Concord Management and Consulting LLC, and Concord Catering which the Mueller report identifies as main sources of IRA funding.[240] The Mueller-produced indictment of the IRA claims that its monthly operating budget at times exceeded $ 1.25 million.[241]

Over the next two years, the IRA's operation changed from one that Mueller characterized as "designed .. to undermine the US electoral system" into a "targeted operation that by early 2016 favored candidate Trump and disparaged candidate Clinton."[242] Utilizing multiple social media platforms, IRA "specialists" had developed a social media network capable of reaching "millions of US persons" by the time the 2016 presidential election took place.[243] When Facebook took down a number of suspected IRA pages in 2017, a representative testified before congress that Facebook estimated the number of people who

237. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 44.
238. Ibid., 43.
239. Ibid., 12.
240. Emily Tamkin, "This Is What $1.25 Million Dollars a Month Bought the Russians," *Foreign Policy*, February 16, 2018, `https://foreignpolicy.com/2018/02/16/this-is-what-1-25-million-dollars-a-month-bought-the-russians/`.
241. United States Department of Justice, *United States v. Internet Research Agency LLC*, 2018.
242. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 4.
243. Ibid.

were served some form of IRA-associated content to be 126 million.[244] The most popular IRA pages included "Secured Borders" , "Being Patriotic" and "Stop All Invaders" .[245]

Despite the novelty of hacking public opinion to sway an election, the Mueller report contains evidence of the hacker tradition alive and well within the new mode: a tendency for playful mischief. Morris made a name for himself with pranks like causing the misspelling of the 'mail' to launch a game, and one of Mr. van Eeden's earliest computer experiences involved the pranking of the Utrecht mainframe managers. Similarly, the Russian trolls seemed unable to resist a little joke of their own. In one of the more heavily redacted sections of the report, the special counsel describes how at the end of May 2016, IRA specialists managed to get a US citizen to hold a sign in front of the White House which read "Happy 55th Birthday Dear Boss".[246] The report, and the indictment of the IRA it cites, indicate that the boss in question was none other than Prigozhin, whose 55th birthday was a few days later on the 1st of June. According to the indictment, the specialists told the sign-bearer that the individual in question "[was] a leader here and our boss . . . our funder."[247] Save the hacker tradition, it is difficult to imagine what purpose such an act could have served. By contrast, the so-called hacking and dumping operations appear devoid of such playfulness.

In the wake of the announcement by the Democratic National Committee (DNC) and cyber security firm CrowdStrike that the DNC had been compromised on June 14th, 2016, it was reported that two disparate actors had been active inside the DNC's networks. CrowdStrike identified them as 'Fancy Bear' and 'Cozy Bear', two Russian advanced, persistent, threat actors associated with Russian intelligence services.[248] Cozy Bear has since been publicly identified by Dutch intelligence as being associated with the Russian Foreign Intelligence Service (SVR),[249] while the Mueller report identifies Fancy Bear as being under the auspices of the Russian Main Intelligence Directorate (GRU). Yet despite

244. United States., *Social Media Influence in the 2016 US. Election, Hearing Before the Senate Select Committee On Intelligence* (Washington: U.S. Govt. Print. Off., November 1, 2017).

245. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 33.

246. Ibid., 19.

247. Justice, *United States v. Internet Research Agency LLC*, 12(b).

248. Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike*, May 15, 2016, `https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/`.

249. Huib Modderkolk, "Dutch agencies provide crucial intel about Russia's interference in US-elections," *de Volkskrant*, January 25, 2018, `https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/?referer=https%3A%2F%2Fwww.google.com%2F`.

the widespread reporting of there having been two Bears inside the DNC and DCCC networks, there is no mention of Cozy Bear in the Mueller report.[250] The report instead identified two individual GRU units as the perpetrators of the hacking and dumping operations directly related to the election meddling Mueller was tasked with investigating. Though the report contains many redactions due to "Harm to Ongoing Matter[s]" (HOM), it seems most likely that it doesn't mention Cozy Bear due to their activities having been outside the scope of Mueller's assignment.[251] Evidence for this position can be found in a recent European Council on Foreign Relations report on the Russian intelligence ecosystem:

"Moscow has developed an array of overlapping and competitive security and spy services. The aim is to encourage risk-taking and multiple sources, but it also leads to turf wars and a tendency to play to Kremlin prejudices."[252]

In such an environment, it is wholly plausible that the two Bears may not have been aware of each other. As early as September of 2016, there was speculation among news outlets and security researchers that Cozy Bear, which according to CrowdStrike had been active inside the DNC's networks since mid 2015[253], was "engaged in traditional espionage"[254] without knowledge of Fancy Bear's activities. Regardless, Mueller's office appears to have determined that their mandate did not cover the operations of Cozy Bear.

Fancy Bear's operations however, fell squarely within their purview. The report identified two 'Military Units' of the GRU, Military Unit 26165 and Military Unit 74455, collectively as Fancy Bear. We hereafter refer to these units as MU2 and MU7 respectively. MU2 primarily targeted the Democratic Congressional Campaign Committee (DCCC), the Democratic National Committee (DNC) and individuals associated with Hillary Clinton's 2016 presidential bid. MU7 released and promoted stolen information, and engaged in offensive operations against US local and state electoral entities, as well as vendors of election-related software.[255]

250. Jeff Stone, "Meet Fancy Bear and Cozy Bear, Russian groups blamed for DNC hack.," *Christian Science Monitor*, May 15, 2016, `https://www.csmonitor.com/World/Passcode/2016/0615/Meet-Fancy-Bear-and-Cozy-Bear-Russian-groups-blamed-for-DNC-hack`.

251. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)."

252. Mark Galeotti, *Putin's hydra: inside Russia's intelligence services* (European Council on Foreign Relations, 2016).

253. Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee."

254. The Economist, "Bear on bear," September 22, 2016, `https://www.economist.com/united-states/2016/09/22/bear-on-bear`.

255. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 36-37.

According to the Mueller report, GRU operations aimed to disrupt the US election began early in March of 2016 when MU2 began a spear phishing campaign against hillaryclinton.com email accounts. Over the course of the month, their campaign expanded to include other domains until they successfully broke into the DCCC network in the first weeks of April using phished credentials.[256] MU2 officers then moved laterally within the DCCC, ultimately compromising 29 hosts. On April 18th, they managed to gain access to the DNC network via a VPN connection between the two networks, and by June 8th had compromised both the DNC's mail and file-sharing servers in addition to several dozen other hosts.[257] During this time, MU2 entrenched themselves, installing surveillance and exfiltration software. By the time their presence was identified, MU2 had managed to steal over 70 gigabytes worth of data from the file-sharing server alone, as well as thousands of emails.[258] The stolen materials included documents and correspondence from the highest ranks of the Clinton organization, including from John Podesta, her campaign manager. Having successfully hacked Democratic party networks, it remained to disseminate the stolen documents.

The GRU's dumping campaign utilized three main vectors: the blog personalities of 'Guccifer 2.0' and 'DCLeaks', and Julian Assange's WikiLeaks. While the DCLeaks persona, including its web presence at dcleaks.com and an assortment of supporting social media profiles, seems to have been used exclusively for disseminating documents, Guccifer 2.0 was also intended to misdirect attention away from the Russian state. Created the day after the DNC and CrowdStrike publicly announced the hack and attributed it to Fancy Bear, Guccifer 2.0's first post tried to take the 'credit' for the DNC hack.[259] According to the Mueller report, Guccifer was intended to be a "lone Romanian hacker" .[260] It seems likely that the GRU's choice of name and nationality was either inspired by, or intended to be conflated with, the real Romanian hacker Marcel Lazăr Lehel. Lehel, who used the pseudonym 'Guccifer', is perhaps best known for revealing the presence of then Secretary of State Clinton's private email server and for distributing a collection of self portraits

256. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 37-38.
257. Ibid., 38.
258. Ibid., 48.
259. Guccifer2, "GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER," May 15, 2016, `https://guccifer2.wordpress.com/2016/06/15/dnc/`.
260. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 42.

painted by George W. Bush.[261][262] Lehel is currently serving a 52-month prison sentence in the US for hacking.[263] His GRU-run namesake eventually posted thousands of DCCC and DNC documents on their blog.[264]

Both the Guccifer 2.0 and DCLeaks personalities were also used to communicate with WikiLeaks. According to the report, DCLeaks attempted to make contact with WikiLeaks on June 24th, 2016, and a week later WikiLeaks initiated contact with Guccifer 2.0. Communications between Guccifer 2.0 and WikiLeaks revealed in the Mueller report and associated indictments indicate that the first WikiLeaks dump of GRU-stolen emails and documents on July 22nd, 2016, was intentionally timed. In a July 6th Twitter direct message (DM) from WikiLeaks to Guccifer 2.0, WikiLeaks wrote "if you have anything hillary related we want it in the next tweo [sic] days preferable [sic] because the DNC is approaching and she will solidify bernie supporters behind her after." In a follow up DM, after estimating Trump's likelihood of winning the presidency at 25% , WikiLeaks continued "..so conflict between bernie and hillary is interesting." The Democratic National Convention began three days after the July 22nd dump.[265]

The next phase of the GRU's election-related hacking activities began five hours after Trump made his now infamous request for foreign assistance: "Russia, if you're listening, I hope you're able to find the 30,000 emails that are missing." Subsequent GRU cyber operations "stole approximately 300 gigabytes of data from [a] DNC cloud-based account." Similarly, within an hour of the infamous Access Hollywood recording of Trump making vulgar comments about women being published by the Washington Post on October 7th, WikiLeaks released the first of a collection of emails stolen from the account of Podesta.[266]

In the direct language typical of the Meuller report, the special counsel summarized their findings: "the Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[267] Given the well substantiated story of information

261. Rachel Weiner and Spencer S. Hsu, "Hacker known as Guccifer sentenced to 52 months in prison," Washington Post, September 1, 2016, https://www.washingtonpost.com/local/public-safety/guccifer-hacker-who-revealed-clintons-use-of-a-private-email-address-sentenced-to-52-months/2016/09/01/4f42dc62-6f91-11e6-8365-b19e428a975e_story.html?utm_term=.fe28ecdcb503.

262. Sam Byford, "George W. Bush's bizarre bathroom self-portraits laid bare by audacious hack," The Verge, February 8, 2013, https://www.theverge.com/2013/2/8/3966678/hacker-reveals-george-w-bush-self-portraits.

263. Mathew J. Schwartz, "Romanian Hacker 'Guccifer' Extradited to US," Bank Info Security, https://www.bankinfosecurity.com/romanian-hacker-guccifer-extradited-to-us-a-11705.

264. Mueller III, "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 43.

265. Ibid., 45.

266. Ibid., 50-58.

267. Ibid., 1.

manipulation and direct hacking told by the Meuller report, considering the 2016 election meddling as a Rubicon crossing seems apt. First, the inertia of tradition is apparent at multiple levels. Within the evolution of the event itself, we see a generally anti-US, election undermining operation develop into a highly specialized and focused hit on Clinton. Considering the hacker tradition demonstrated by the birthday sign and the basis for the event apparent in Russia's 2014 Ukrainian operations, it is clear that the ideas and forms used didn't spring fully-formed from nowhere. Secondly, the boldness with which the Russian operatives like Fancy Bear pursued their objectives is indeed suggestive of a point of no return. The meddling inched the Pandora's box of cyber-conflict ever so slightly farther open, and indeed Weinstein's Rubicon invocation was in the context of what appears to be an increasingly offensive cyber posture on the part of the US.[268]

9.2 Securitization

As of this writing, the Mueller report is less than two months old and full of HOM redactions. Yet already we see clear similarities with our previous cases. One such similarity is in terms of what appears to be a collective loss of innocence on the part of national populations. The attempts made by the Russian state over the last five years have "plausibly worsened a general sense of paranoia, doubt, and confusion among people who were increasingly unsure of what their fellow citizens believe[]" according to a recent work by Henry Farrell and Bruce Schneier titled *Common-Knowledge Attacks on Democracy.*[269] Farrell and Schneier interpret this as an attack on the distinction between "common" and "disputed" knowledge, which they identify as a democracy's attack surface. Briefly, common knowledge is the body of knowledge shared by an entire society required for the healthy functioning of the polity. Common knowledge in a democracy, for instance, includes the understanding that the results of an election are sacred, or a ubiquitous understanding that, regardless of outcome, the participants will respect the results. Such universally shared understandings establishes the framework within which the population can engage in debate over disputed knowledge, which in a democracy includes issues like whether or not the nation should declare war or raise taxes. Before returning to the perhaps more obvious connection between this ontology and attack surface expansion,

268. Sanger, "Utilities Cautioned About Potential for a Cyberattack."
269. Farrell and Schneier, "Common-Knowledge Attacks on Democracy."

we will first address how it provides a basis for understanding the election meddling as representative of a loss of innocence.

In mid 2016, Adrian Chen summed up a Russian activist's understanding of their government's trolling operations as intended "not to brainwash readers but to overwhelm social media with a flood of fake content, seeding doubt and paranoia, and destroying the possibility of using the Internet as a democratic space."[270] In order to destroy the possibility of using the Internet as a democratic space requires it to have already been thusly framed. Similarly, on May 29th of this year, lawyers for Facebook asserted that "there is no privacy interest [on Facebook], because sharing with a hundred friends on a social media platform .. negate[s] any reasonable expectation of privacy." [271] While Facebook is not under fire for the destruction of a democratic space, they too are combating latent assumptions as to what the Internet is, and how it should work. However bizarre the notion that information freely shared via a commercial platform is somehow subject to the same legal rules which, for instance, govern information coerced from individuals by the state, the idea is widely held. This is clear from the growing public anger toward Facebook, especially in the wake of incidents like Cambridge Analytica.[272] Where the 2016 election meddling served to quickly demonstrate the limitations of the Internet as a democratic space, Facebook's "issues" with privacy have demonstrated fundamental problems with assuming the Internet is a simple extension of the analog world, especially with respect to privacy. As the Facebook saga demonstrates, we are collectively experiencing a loss of innocence with regard to privacy on the Internet. The 2016 election meddling served as a fast-acting catalyst for a similar loss of innocence with regard to the potentially utopian uses of the Internet for democratic purposes in much the same way the 2007 attack on Estonia tarnished ideals of utopian Internet-governance.

In the aftermath of the election meddling, we see the emergence of the same exclusionary reaction of Estonia to the attacks on their structures and processes. Perhaps even more dramatically than in Estonia's case, there is no greater authority the US can turn to which is capable of establishing and enforcing international rules. Despite this, we have already seen the US take two major exclusionary steps: the take-down of foreign-influence pages

270. Adrian Chen, "The Real Paranoia-Inducing Purpose of Rusian Hacks.," The New Yorker, July 27, 2016, `https://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks`.

271. (!! how do I CITE p. 7 of the may 29 FB litigation) US District Court, Northern District of California. "In RE: Facebook, Inc. Consumer Privacy User Profile Litigation." May 29, 2019. San Francisco. p.7

272. Issie Lapowsky, "How Cambridge Analytica Sparked the Great Privacy Awakening," Wired, March 17, 2019, `https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/`.

on social media combined with improved detection and removal processes[273], and the development of improved deterrent measures.[274] In April of this year, the US also indicted Julian Assange, and looks poised to successfully extradite him from London where he had been living in asylum in the Ecuadorian embassy.[275] Though he was sought in the US on charges related to the disclosure of materials to do with the wars in Iraq and Afghanistan, his arrest may also represent the US flexing its international weight, much like the Estonian headquartering of the CCDCOE and it's publication of the Tallinn Manuals demonstrated Estonia's cyber acumen.

Also very much in keeping with the Estonian event is the aforementioned expansion of attack surface represented by the 2016 election meddling. Though the Russians had attacked elections before, 2016 was the first time they targeted them in a grassroots fashion. In their 2014 attempt to subvert elections in Eastern Ukraine, the Russians employed tactics against social media which would have worked against more traditional, non-social media as well. In 2016 however, their attack utilized as a vector the user-generated content component of social media which truly distinguishes it from traditional forms. In doing so, a nation's attack surface was extended to include its ability to produce authentic, public consensus. As the Russian activist attested to, this vector allowed them to effectively "widen contested political knowledge so that it spill[ed] over into disagreements over the common political knowledge that democracy needs to operate."[276] By legitimizing the idea of fake news, the Russians functionally undermined common knowledge by moving the news media's general ability to report facts from the common into the disputed. The combination of Trump's recent refusal to believe even his own pollster's conclusions that he currently trails his democratic rivals[277], and his 2016 suggestion that he would only accept the results of the presidential election if he won[278], powerfully evidence the danger of the newly expanded attack surface and the success of the Russian operation.

273. Jenna Mclaughlin and Donnie O'Sullivan, "Lacking direction from White House, intelligence agencies scramble to protect midterm elections from hackers," CNN, July 27, 2018, `https://edition.cnn.com/2018/07/27/politics/agencies-midterms-election-security/index.html`.

274. Sanger and Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid."

275. Charlie Savage, Adam Goldman, and Eileen Sullivan, "Julian Assange Arrested in London as U.S. Unseals Hacking Conspiracy," *The New York Times*, April 11, 2019, `https://www.nytimes.com/2019/04/11/world/europe/julian-assange-wikileaks-ecuador-embassy.html`.

276. Farrell and Schneier, "Common-Knowledge Attacks on Democracy."

277. Bess Levin, "Trump "Purges" Pollsters who Revealed He's Losin to Biden," *Vanity Fair*, May 17, 2019, `https://www.vanityfair.com/news/2019/06/trump-fires-pollsters`.

278. Patricia Zengerle and Emily Stephonson, "Trump says he will accept election result - if he wins," *Reuters*, October 19, 2016, `https://www.reuters.com/article/us-usa-election/trump-says-he-will-accept-election-result-if-he-wins-idUSKCN12J0ZM`.

That success, combined with the fact that incidents like the 2008 Estonian attacks and the 2014 Ukrainian election meddling were also clearly interactions between emerging cyber capabilities and democratic processes, is strong evidence for the Rubicon-like nature of the 2016 election meddling. The republic, to a degree, endured Marius and Sulla and a host of other anti-republican forces, but not the civil war Cesar precipitated when he entered Italy with the 13th Legion. Yet however disastrous certain parties may find the effects of the IRA and GRU activities, their actions over the last four years have attracted the attention of a broad group of interests to the digital problems of a "post-fact" world.[279] One such view comes from Danah Boyd, founder of the Data & Society research institute and Principal Researcher at Microsoft Research, who delivered the keynote address at last year's SXSW EDU conference. Speaking to an audience of largely educators, Boyd framed the Farrell and Schneier's common vs. disputed distinction in terms of gas lighting - a term originating from a 1938 play about domestic abuse which has come to describe manipulation designed to cause the victim to question their own faculties.[280][281]

Boyd contests that "the most dangerous [problem in our media landscape] is how it's being weaponized to gaslight people, to make them feel like they can't tell what reality is."[282] She made this claim within the context of the so-called "pizzagate" and "crisis-actor" conspiracies, both of which were amplified by media coverage which factually negated them.[283] Though a man did show up at a Washington DC pizza parlor with a gun, and despite the fact that Parkland survivors must often defend themselves against claims that they are in fact paid actors, neither gaslit narrative had lethal effect.[284] Measles, however, has already killed more people in the US this year alone than it did in 1994, six years before it was declared eliminated.[285] The concept of gaslighting, as wielded by Boyd revolves around the same vector for undermining a democratic polity that Farrell and

279. Francis Fukuyama, "The Emergence of a Post-Fact World," *Project Syndicate*, January 12, 2017, https://www.project-syndicate.org/onpoint/the-emergence-of-a-post-fact-world-by-francis-fukuyama-2017-01.

280. Danah Boyd, "What Hath We Wrought?" (SXSW EDU, Austin TX, March 7, 2018).

281. Ben Yagoda, "How Old Is 'Gaslighting'?," *The Chronicle*, January 12, 2017, https://www.chronicle.com/blogs/linguafranca/2017/01/12/how-old-is-gaslight/.

282. Boyd, "What Hath We Wrought?"

283. Ibid.

284. Merrit Kennedy, "'Pizzagate' Gunman Sentenced To 4 Years In Prison," *NPR News*, May 22, 2017, https://www.npr.org/sections/thetwo-way/2017/06/22/533941689/pizzagate-gunman-sentenced-to-4-years-in-prison.

285. US Center for Disease Control and Prevention, "U.S. measles cases in first five months of 2019 surpass total cases per year for past 25 years," CDC, May 30, 2019, https://www.cdc.gov/media/releases/2019/p0530-us-measles-2019.html.

Schneier's delineation between common and disputed knowledge does: the destruction of consensus.

Perhaps one of the most fundamental points Boyd made in her talk was to do with what she describes as a "prioritiz[ation of] individual agency" through "the narrative of media literacy as the solution to misinformation."[286] Teaching students to critically interrogate the information they encounter, according to Boyd, played into a narrative which holds the media and institutions of higher education as trying to exert an "authority over epistemology."[287] Farrell and Schneier make a similar point, citing, for instance, "disparities of political influence between rich and poor" as being fundamental to the "contestation and political debate" required for the healthy function of a democratic polity.[288] From very different perspectives, both make the point that growing disparities in perceived and real power are damaging that healthy function. Both their points could easily be conceived of as an increasing lack of moral restraint on the part of many parties, and the widespread (though varied in form) perception of looming tragedy. It is perhaps too early to consider such a beginning indicative of coming securitization, but in the context of this work, the suggestion is difficult to ignore.

286. Boyd, "What Hath We Wrought?"
287. Ibid., ∼19:00.
288. Farrell and Schneier, "Common-Knowledge Attacks on Democracy."

10

Conclusion

10.1 Old Forms, New Technology

Through each of our events, we have attempted to trace the interaction of pre-digital, or traditional, forces and digital-age technology. We have used the concept of the tragedy of the commons as a frame for both the entire process of securitization, as well as a mechanism to understand how the first component, that of tragedy, may manifest. We have also utilized the phenomenon of exclusion, and its natural corollary of 'othering' whatever entity, action or idea was excluded, in much the same way. In addition to these obviously field-agnostic concepts, we have also utilized the cyber-security phenomenon of threat-modeling and attack surfaces in two ways. Not only do they serve to tie our exploration more tightly to its computing context, but through their continued use, their true, abstract, field-spanning nature emerges, and reinforces the fact that computer security doesn't exist in a vacuum. Having now covered six events which span the entire digital age, we may now consider securitization over time.

In the passage of the FCRA, we saw market forces raise barriers where none had previously existed. Combined with an emerging fear of dehumanization through the implementation of early computing technology, this newly introduced exclusion irritated the US public to the point where they sought to implement exclusionary measures of their own. What they perceived as the inevitable end of the old mode - in this case the traditional, word-of-mouth SCMs - clearly involved the perception that an idealized, pure-public-like good wasn't going to last in the face of total laissez-faire. For fear of an uncontrolled slide away from that ideal, the well-established tradition of government intervention through legislation, in response to public outcry, securitized the upstart CRAs.

While the story of Morris' worm involved much heavier use of computing technology than occurred during the 1960s, the event follows the same pattern. The worm demonstrated that in fact the Internet, idealized as it often was as a pure-public good, or commons-like, was in fact quite rivalrous. Further, his worm attached a price tag to network insecurity, finally capturing the attention of business interests many of whom had remained recalcitrant toward a security-first computing doctrine throughout the 80s.[289] Though the tragedy that took place in the digitally-enabled space of the Internet took place at digital speeds, ultimately, securitization fell back on the same paradigm for regulation seen in the passage of the FCRA. Exclusion was implemented by the government.

Concurrently with Morris' worm, the CWI's computing department was experiencing a very slow securitization, largely thanks to the lack of a Morris-level event. The CWI's well-financed, agile nature, and its leadership's protection of its members' penchant for pure exploration seems to have allowed it to exist at the cutting edge of technological development without being wholly subjected to the pressures of the business-political powers, despite these existing in force. This relative calm allowed the CWI's staff time to adjust more naturally than was the case for the American Internet community in the face of Morris' worm, and as such, there is not as obvious a point of tragedy. Despite no clear singular event to point to, the encapsulation of security within a physical structure was an 'old way', and its inevitable updating as computing dissipated across networks and into PCs fits cleanly our pattern of developing impurity as tragedy. Over time, the CWI was required to implement increasingly distributed forms of security, and evidence for these exclusionary actions can readily be found in the CST Bulletins, as well as in the testimony of CST members. The interaction of old-form and new-technology most apparent here is the tradition of facilities-encapsulated security and the distributing force of networks.

Just a few years after the Morris worm, as the CWI was dealing with increasingly distributed access to their facilities, Mr. van Eeden experienced surprise rivalry in his utopian, digitally-enabled Metro. Compared to previous events, the Metro was relatively small, but it represented a distinctly new space which at the time of its creation had yet to be securitized. The most obvious, and likely powerful tradition at play in this event, the highly authentic hacker-ethos of Mr. van Eeden, lead directly to the idealization of the Metro as pure-public. Yet very quickly, what we might now describe as something between trolling and hate-speech (neither of which, sans labels, are modern phenomena), demonstrated the distance between that idealization and the reality of the space: the Metro was in fact rivalrous. Further, its carrying capacity for those lacking in moral restraint

289. Courtney Jr, "Untitled."

was quite low. Lacking any tradition of authority save perhaps that of a dictator, Mr. van Eeden fell back on his pragmatic background and implemented exclusion much as a parent would. The securitization of the Metro therefore was a result of what turned out to be the high rivalry of such online spaces, the limit-seeking tradition Mr. van Eeden embodied, and a pragmatic need to sustain the space.

In 2007 Estonia, the emancipation of security from facilities seen at the CWI, along with the digitally-enabled spaces of the Metro and Morris collided with a very strong tradition of international enmity. Like in prior events, the revelation that digitally enabled, utopian projects weren't as pure-public as they were idealized to be resulted in a perception of tragedy. However unlike previous events, not only were the resources of e-governance not physically constrained, but access to those resources wasn't even constrained by national borders. In spite of this, Estonia, by appealing to the traditions of cooperating with the West and of deterrent building, as well as utilizing modern technical solutions did succeed in excluding some Russian behaviors.

Finally, in 2016, the basis upon which the US democratic system functions was attacked. Using novel technical vectors to malign public opinion and undermine consensus building, Russian agents demonstrated that the precepts of democracy were targetable, and vulnerable. In response to the clearly tragic need to define rules in a space that had previously functioned without them, the US has so far largely followed the Estonian model. Exclusionary action has been taken within social media designed to better identify and remove foreign agents and hate speech. In parallel, the US has begun to demonstrate that it not only possess cyber weapons, but that it may in fact be willing to use them in response to threat. A deterrent is only effective if your opponent can't be sure you won't use it, and by demonstrating that potential, the US functionally excludes some Russian meddling behavior.

10.2 Corroborating The Value of Diversity

A broad conclusion of this work has to do with the value of relatively non-technical approaches to solving problems in spaces that may not only be traditionally considered technical, but that may themselves be enabled through high technology. The Metro and the Internet are both examples of such spaces. By attempting to do precisely what the computer security field is now increasingly appreciating the need for - holism - we have arrived at much the same conclusions that the field did through more technical means. Additionally, the use of the concepts of attack surface and threat modeling served to reinforce

the parallels between computer security and various other combative spaces. Specifically, military affairs has already collected the WSS idea of holism within its own frame, and labeled it RMA. The use of this parallel helps underscore the value of our approach.

In the passage of the FCRA we saw traditional forces result in a tragedy which was addressed in a straightforward manner through the storied process of legislation in response to public outcry. During this same time, Ware was discussing computer security around the water cooler, and viewed it as valuable to people only in so far as it was valuable to the organs of national security upon which those people directly relied for safety.[290] Together, this represents our beginning: securitization well within established parameters, and computer security in an almost exclusively military-oriented frame. Given the threats of the day, these both worked fine.

The 1970s saw two updates occur. The Soviets began developing the concept of what would become RMA, and computing transitioned away from the mainframe model toward a more decentralized network and PC-oriented form. By the early 1980s these models began to overlap: WarGames literally depicted the interaction between a networked teenager and the military's ultimate weapon. No longer was computing valuable to people simply because it was valuable to the nation's defense structures, but it was valuable in its own right. Email, which began being developed commercially during the 1980s was the first killer app.[291] The decade saw, as happened at the CWI, the emancipation of security from facilities, and as a result the emancipation of security from a single authority. RMA-style thinking, which was becoming more popular at this time in the US, held that advances in tactical ability driven by technology were valuable only in so far as they were distributed throughout all supporting structures. The general who tried to reassure the public as to the infeasibility of the so-called WarGames scenario by saying that was always a "man .. in the loop" was perhaps more prescient than he intended.[292]

While the CWI played out the distributing of security concerns, Morris and Hess collectively represented the growing schism between traditional, top-down military-oriented ways of thinking and new, distributed models. Hess, a cold warrior convicted of espionage, engendered little to no debate as to the merits of his actions. There was little reason to rehash a functioning tradition. Morris on the other hand represented the new distributed, physically-emancipated threat for which *little* tradition existed. As such, his worm sparked a fierce debate between the old guard of the DoD and FBI, and the new guard of academic,

290. Ware, *Oral history interview with Willis Ware*.
291. Glossbrenner and Glossbrenner, *The complete handbook of personal computer communications*.
292. News, "World News Tonight."

hacker, and UNIX cultures. Yet despite a clearly emergent new form, some aspects of the old remained.

Most strikingly, though the Internet was a technologically-enabled space, and as such new in form, its structure lent itself to traditional forms of authority. It was the Department of Justice who prosecuted Morris, and the FBI who investigated him. Partially by virtue of his actions being wholly contained within the US, there remained an FCRA-like pattern for tragedy resolution to follow. Similarly, despite Mr. van Eeden's Metro also being a technologically-enabled space, it too lent itself to the old mode of authoritarianism. Despite Mr. van Eeden's bona fide hacker status, he implemented top-down rules much in keeping with the tradition of the FCRA and Morris, albeit more pragmatically. It was during this same early-90s period that the US Desert Storm operation resoundingly demonstrated the effectiveness of a technology-heavy RMA doctrine, setting a precedent for the next thirty years.

It is in Estonia in 2007 that we see the next large break from tradition. In their response to perceived tragedy, Estonia lacked a traditional authority anywhere near as all-powerful or all-encompassing as the US federal government represented in our earlier events. It was the Estonian equivalent that was attacked. They therefore lacked a tradition to appeal to in guiding their response, and in their successful implementation of exclusion we see an early convergence of RMA and computer security - pre WSS 2008. In addition to othering Russia as much as possible by both setting up the CCDCOE, and through closer cyber cooperation with NATO, they also took to heart the very RMA-like notion of tactical advances only being as valuable as accompanying advances in their supporting structures. Their digital governance operations, technically advanced as they were, required similarly advanced underpinnings. The Estonian doubling-down on cyber-security initiatives targeted at their general public serves as powerful evidence for their appreciation of this fact.[293] Finally, Estonia's size and international weight places the event in a more transitionary position than a similar event undergone by, for instance, a member of UN Security Council. There were indeed larger entities to whom Estonia might have appealed, however the presence of their chief antagonist on that council would likely have rendered such an appeal useless.

Reaching the present day, the US election meddling was *fully* emancipated from the tradition of ready-made authorities. Like all the other events, the collective perception of tragedy was fairly straightforward; it turned out that the borders of common knowledge were in fact not sacred. However much more completely than Estonia in 2007, the US of

293. E-Estonia, "Proactive governance enhances service delivery in Estonia," *E-Estonia*, May 2019, `https://e-estonia.com/proactive-services-estonia/`.

today wholly lacks a supra-national authority capable of implementing top-down exclusion. Like Estonia, the US has implemented some forms of exclusion, as we have seen, but ongoing Russian meddling suggests there is a way to go yet. And here, with the CWI's transition from facility-enshrined security model to distributed security model in mind, we perceive the value of RMA thinking applied to digital security.

In 2008, when the WSS set out their goal of better bridging the gap, both theoretical and practical between a technology and its implementation, they called for RMA-style thinking. Not only was it valuable to develop high-end tactical abilities, like those showcased in top systems security journals, but it was equally important to develop improved implementations much like Simko's work embodies. Given the heterogeneity represented by Xu's systems theory and Simko's humanism, the computer security field appears to be moving in an RMA-like direction. This movement toward many-level diversity, from technical development to implementation, is indicative of a gap between the real threat, and perceived threat. The recent election meddling and the continued prevalence of increasingly destructive cyber attacks further evidences this divide. Schneier and Farnell's paper draws a very similar conclusion by highlighting the need to consider computer security through the lens of national security: a gap closing measure.

Another way to look at this disconnect, which RMA-style doctrine looks to close, is as the disparity between technology and threat-model we have so often seen result in disaster. The pre-WWI French Army doctrine that lead to the deaths of so many soldiers, the threat-model of the bored student that Morris destroyed, and early 21st century threat-modeling which failed to take into account the nation-state, all fit the pattern. Similarly, the gap between the true, and commonly-accepted attack surface of some system is demonstrative of the same lack of holism. Despite the somewhat Rumsfeldian implications of there being a disparity between what we know and what's 'real', it is undeniably dangerous to disregard a well established pattern. Especially one which has repeatedly resulted in tangible harm.

Our work here can now be seen as corroborating the value of diversity in approach to solving security issues which the computer security field has already to a degree embraced, having developed it through the fairly traditional and technically-oriented action of experts meeting at a conference. By reaching a similar conclusion through a humanistic and historical exploration of computer security, we have demonstrated the value of such an approach in what's often considered to be a highly technical field. Further, by considering cyber-security notions like those of attack surfaces and threat modeling abstractly, we have demonstrated the value of field-crossing exploration. The similarity between our

work reinforcing the value of diversity, and the military affairs concept of RMA both support the WSS contention that both implementation and tactical development are equally important.

10.3 Going Forward

The history of computer security, as depicted through the events laid out here, suggests a trend which may have interesting implications for the inevitable future development of new spaces, and their eventual securitization. Since the 1960s the authorities which implement the exclusion critical to securitization have, generally, grown from intra-national units, like individuals and civil governments, to international units like NATO. In the absence of a readily available authority, novel forms of exclusion have been implemented which have, as of yet, been in keeping with the available traditions. Estonia tightened their cooperation with NATO in accordance with their historically antagonistic relationship with Russia. The US, which since WWII has maintained an enormous stockpile of military resources, including nuclear weapons, has, at least in part, kept up this practice by attempting to implement exclusion through deterrent measures. However we now see the development of spaces for which no such long-standing traditions exist.

From the FCRA to 2016, the nature of the spaces undergoing securitization have become decidedly less traditional. Where securitizing the CRAs of the 1960s was obviously a job for Congress, it was quite unclear what body should implement exclusion on a global Internet. This trend, for our purposes, culminated in 2016. The incredible heterogeneity of social media participants lends itself less to a single, prescriptive tradition than any of the previously securitized spaces. Combined with there being no obvious single authority understood by a majority of Internet users as rightly capable of excluding rivalrous behavior, modern cyber securitization presents a particular challenge.

Another possible implication of securitization lacking tradition is that, given the typically tight relationship between forms of exclusion and tradition, it is wholly possible that 'unnatural' means of exclusion (i.e. those not in keeping with tradition) will prove less effective, or even counter productive in the eyes of the space's users whose traditions were not followed. Social media and the Internet more broadly, as a democratic space, is one which necessarily combines many disparate views. Democratic debate is, when healthy, a point of interaction for a host of varied traditions, and as such the securitization of it is likely resistant to simple tradition-following modes of exclusion. In the face of

ever growing distributed spaces, and the related increasing heterogeneity of those spaces, tradition-agnostic approaches may need to be found.

This emancipation of spaces from both tradition and authority presents unique problems for the securitization of global, distributed spaces like social media, and the Internet at large. However considering the value of diversity evidenced here from multiple angles and in many different forms, it is hard not to imagine that that same diversity of tradition which suggests problems for the implementation of exclusion is not also in some way a silver lining. The increasingly diverse spaces enabled by technological development, should they take on diversity-embracing traditions of their own, likely represent powerful and effective bases for future forms of exclusion.

Sources

Interviews

Dick Bulterman. Interview took place on the July 4, 2019, in Mr. Bulterman's office at the Vrije Universiteit (VU), Amsterdam. Mr. Bulterman is currently a fellow at the Centrum Wiskunde & Informatica (CWI), and the Director of Research Schools at the VU. This interview focuses on his time as the Head of Computer Systems and Telematics (CST) at the CWI.

Daniel Karrenberg. Interview took place on the June 26, 2019, at the RIPE NCC offices located within Amsterdam's Central Station where Mr. Karrenberg is the Chief Scientist. Interview focused on Mr. Karrenberg's early experiences with computing and networking leading up to, and through his time at the CWI CST in the late 1980s and early 1990s.

Michael van Eeden. Interview with Michael van Eeden on June 25, 2018, in Mr. van Eeden's residence and work shop at Roomolenstraat 1-R, Amsterdam. The interview focused on Mr. van Eeden's early experiences with computing and hacking, up through his time as an administrator in the Amsterdam Digital City project of the 1990s and 2000s.

Bibliography

Abbate, Janet. *Inventing the internet*. MIT press, 2000.

Abella, Alex. *Soldiers of reason: The RAND corporation and the rise of the American empire*. Houghton Mifflin Harcourt, 2009.

Alexander, David. "Theft of F-35 Design Data Is Helping US Adversaries—Pentagon." *Reuters, June* 19 (2013).

Alexander, Michael. "High-tech boom opens security gaps." *Computerworld* 24, no. 14 (1990): 118–119.

Alperovitch, Dmitri. "Bears in the Midst: Intrusion into the Democratic National Committee." *CrowdStrike*, May 15, 2016. `https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/`.

Aurigemma, Salvatore, and Thomas Mattson. "Effect of long-term orientation on voluntary security actions." *Information & Computer Security* 27, no. 1 (2019): 122–142.

Avineri, Shlomo. "War and Slavery in More's Utopia." *International Review of Social History* 7, no. 2 (1962): 260–290.

Beertema, Piet. "Piet Beertema's web site." 2019. `https://godfatherof.nl/`.

Berners-Lee, Tim, and Mark Fischetti. *Weaving the Web: The original design and ultimate destiny of the World Wide Web by its inventor*. DIANE Publishing Company, 2001.

Boyd, Danah. "What Hath We Wrought?" SXSW EDU, Austin TX, March 7, 2018.

Bruijne, Mark de, Michel van Eeten, Carlos Hernández Gañán, and Wolter Pieters. *Towards a new cyber threat actor typology*. Technical report. Delft University of Technology, 2017.

Bulterman, Dick. *Interview*, July 4, 2019.

Buzan, Barry, Ole Wæver, Ole Wæver, and Jaap De Wilde. *Security: A new framework for analysis*. Lynne Rienner Publishers, 1998.

Byford, Sam. "George W. Bush's bizarre bathroom self-portraits laid bare by audacious hack." The Verge. February 8, 2013. https://www.theverge.com/2013/2/8/3966678/hacker-reveals-george-w-bush-self-portraits.

Campbell-Kelly, Martin. *Computer: A History of the Information Machine*. Routledge, 2018.

Cardenas, Alvaro A, Tanya Roosta, and Shankar Sastry. "Rethinking security properties, threat models, and the design space in sensor networks: A case study in SCADA systems." *Ad Hoc Networks* 7, no. 8 (2009): 1434–1447.

Ceruzzi, Paul E, and William Aspray. *The Internet and American Business*. MIT Press, 2008.

Chen, Adrian. "The Real Paranoia-Inducing Purpose of Rusian Hacks." The New Yorker. July 27, 2016. https://www.newyorker.com/news/news-desk/the-real-paranoia-inducing-purpose-of-russian-hacks.

Coates, Joseph F. "The Future of Data Security." *COMP. SECURITY J.* 2, no. 1 (1983).

Computer Networks - The Heralds Of Resource Sharing. International Conference on Computer Communications, 1972.

Courtney Jr, Robert H. "Contemporary data security: A leadership vacuum." *COMP. SECURITY J.* 4, no. 2 (1986): 7–16.

———. "Untitled." 11th Annual Computer Security Applications Conference, December 1995.

CWI. *Annual Report '83*. Centrum voor Wiskunde en Informatica.

———. *Annual Report '87*. Centrum voor Wiskunde en Informatica.

———. *Annual Report '88*. Centrum voor Wiskunde en Informatica.

Cybersecurity and Infrastructure Security Agency. "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)." 2014. https://www.us-cert.gov/ics/alerts/ICS-ALERT-14-281-01B.

Davies, Howard, and Beatrice Bressan. *A history of international research networking: The people who made it happen*. John Wiley & Sons, 2010.

Del Monte, Louis A. *Nanoweapons: A Growing Threat to Humanity*. U of Nebraska Press, 2017.

Delivorias, Angelos. "Understanding Securitisation: Background, Benefits, Risks." *European Parliament Research Service, PE569* 17 (2016).

Dibbell, Julian. "A rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society." *Ann. Surv. Am. L.*, 1994, 471.

Disease Control, US Center for, and Prevention. "U.S. measles cases in first five months of 2019 surpass total cases per year for past 25 years." CDC. May 30, 2019. https://www.cdc.gov/media/releases/2019/p0530-us-measles-2019.html.

Dupont, Benoit. "Cybersecurity futures: How can we regulate emergent risks?" *Technology Innovation Management Review* 3, no. 7 (2013).

E-Estonia. "Proactive governance enhances service delivery in Estonia." *E-Estonia*, May 2019. https://e-estonia.com/proactive-services-estonia/.

———. "The Guardian: Estonia "rapidly transformed from a Soviet state to digital utopia"." *E-Estonia*, September 2016. https://e-estonia.com/the-guardian-estonia-rapidly-transformed-from-a-soviet-state-to-digital-utopia/.

———. "We have built a digital society and so can you." https://e-estonia.com/.

Economist, The. "Bear on bear." September 22, 2016. https://www.economist.com/united-states/2016/09/22/bear-on-bear.

Eeden, Michael van. *Interview*, June 25, 2018.

Eisenberg, Ted, David Gries, Juris Hartmanis, Don Holcomb, M Stuart Lynn, and Thomas Santoro. "The Cornell commission: on Morris and the worm." *Communications of the ACM* 32, no. 6 (1989): 706–709.

Farrell, Henry, and Bruce Schneier. "Common-Knowledge Attacks on Democracy." *Berkman Klein Center Research Publication*, nos. 2018-7 (2018).

Fukuyama, Francis. "The Emergence of a Post-Fact World." *Project Syndicate*, January 12, 2017. https://www.project-syndicate.org/onpoint/the-emergence-of-a-post-fact-world-by-francis-fukuyama-2017-01.

Furletti, Mark J. "An overview and history of credit reporting." *Available at SSRN 927487*, 2002.

Furnell, Steven, and Nathan L. Clarke. "Guest editorial." *Information & Computer Security* 26, no. 3 (2018): 262–263. doi:10.1108/ICS-06-2018-0065. https://doi.org/10.1108/ICS-06-2018-0065.

Galeotti, Mark. *Putin's hydra: inside Russia's intelligence services*. European Council on Foreign Relations, 2016.

Gartner, Scott Sigmund, and Marissa Edson Myers. "Body counts and" success" in the Vietnam and Korean Wars." *The Journal of Interdisciplinary History* 25, no. 3 (1995): 377–395.

Gervais, Michael. "Cyber attacks and the laws of war." *Journal of Law & Cyber Warfare* 1, no. 1 (2012): 8–98.

Ghai, Rohit. "Cybersecurity Silver Linings." RSA Conference 2018, 2018.

Glossbrenner, Alfred, and Alfred. Going online Glossbrenner. *The complete handbook of personal computer communications*. St. Martin's Press, 1990.

Graham, Paul. "The Submarine." 2005. `http://www.paulgraham.com/submarine.html`.

Guccifer2. "GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER." May 15, 2016. `https://guccifer2.wordpress.com/2016/06/15/dnc/`.

Hafner, Katie, and John Markoff. *Cyberpunk: outlaws and hackers on the computer frontier, revised*. Simon / Schuster, 1995.

Hammersley, Ben. "Concerned about Brexit? Why not become an e-resident of Estonia." *Wired*, March 27, 2017.

Hanson, Victor Davis. "Office Hours: VIctor Davis Hanson on NATO." PolicyEd. 2018. `https://www.policyed.org/intellections/nato-21st-century-ensuring-liberal-democracy-europe/video-0`.

Hardin, Garrett. "The tragedy of the commons." *Science* 162, no. 3859 (1968): 1243–1248.

Harry, Charles, and Nancy Gallagher. "Classifying Cyber Events: A Proposed Taxonomy." *Journal of Information Warfare* 17, no. 3 (2018): 17.

Henrotin, Joseph. *The Art of War in the Network Age: back to the future*. Vol. 1. Wiley Online Library, 2016.

Hosseinzadeh, Shohreh, Sampsa Rauti, Samuel Laurén, Jari-Matti Mäkelä, Johannes Holvitie, Sami Hyrynsalmi, and Ville Leppänen. "Diversification and obfuscation techniques for software security: A systematic literature review." *Information and Software Technology*, 2018.

Howard, Michael, Jon Pincus, and Jeannette M Wing. "Measuring relative attack surfaces." In *Computer security in the 21st century*, 109–137. Springer, 2005.

Hoy, JB, MT Brewer, BA Peterson, and G Dittmer. *Computer Security: Virus Highlights Need for Improved Internet Management*. Technical report. GENERAL ACCOUNTING OFFICE WASHINGTON DC INFORMATION MANAGEMENT AND . . ., 1989.

Justice, United States Department of. *United States v. Internet Research Agency LLC*, 2018.

Kaplan, Fred. *Dark Territory: The Secret History of Cyber War*. Simon / Schuster, 2016.

Karrenberg, Daniel. *Interview*, June 26, 2019.

———. "Password Security." *CST Bulletin*, 1990.

Kennedy, Merrit. "'Pizzagate' Gunman Sentenced To 4 Years In Prison." *NPR News*, May 22, 2017. https://www.npr.org/sections/thetwo-way/2017/06/22/533941689/pizzagate-gunman-sentenced-to-4-years-in-prison.

Keys, Benjamin J, Tanmoy Mukherjee, Amit Seru, and Vikrant Vig. "Did securitization lead to lax screening? Evidence from subprime loans." *The Quarterly journal of economics* 125, no. 1 (2010): 307–362.

Kingsley, Patrick. "How tiny Estonia stepped out of USSR's shadow to become an internet titan." *The Guardian*, May 15, 2012.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Jenny Oberholtzer, et al. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Rand Corporation, 2017.

Landau, Susan. *Listening In: Cybersecurity in an Insecure Age*. Yale University Press, 2017.

———. "Making sense from Snowden: What's significant in the NSA surveillance revelations." *IEEE Security & Privacy* 11, no. 4 (2013): 54–63.

———. "The Second Crypto War - What's Different Now." In *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, 2018. ISBN: 978-1-939133-04-5. https://www.usenix.org/conference/usenixsecurity18/presentation/landau.

Lander, Mark, and John Markoff. "In Estonia, what may be the first war in cyberspace." *New York Times*, May 28, 2007.

Langman, Peter. "Role models, contagions, and copycats: An exploration of the influence of prior killers on subsequent attacks." *Available on www. schoolshooters. info*, 2017.

Lapowsky, Issie. "How Cambridge Analytica Sparked the Great Privacy Awakening." Wired. March 17, 2019. https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/.

Lévesque, Fanny Lalonde, Sonia Chiasson, Anil Somayaji, and José M Fernandez. "Technological and human factors of malware attacks: A computer security clinical trial approach." *ACM Transactions on Privacy and Security (TOPS)* 21, no. 4 (2018): 18.

Levin, Bess. "Trump "Purges" Pollsters who Revealed He's Losin to Biden." *Vanity Fair*, May 17, 2019. https://www.vanityfair.com/news/2019/06/trump-fires-pollsters.

Lipner, Steven B. "The birth and death of the orange book." *IEEE Annals of the History of Computing* 37, no. 2 (2015): 19–31.

Lloyd, William Forster. *Two Lectures on the Checks to Population: Delivered Before the University of Oxford, in Michaelmas Term 1832*. JH Parker, 1833.

Lubar, Steven. ""Do Not Fold, Spindle or Mutilate": A Cultural History of the Punch Card." *Journal of American Culture* 15, no. 4 (1992): 43–55. doi:10.1111/j.1542-734X.1992.1504_43.x. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1542-734X.1992.1504_43.x. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1542-734X.1992.1504_43.x.

Author of Computer 'Virus' is son of NSA expert on data security., 1988, A1.

Marsan, Carolyn Duffy. "Where is Robert Morris now?" Network World. 2008. https://www.networkworld.com/article/2268914/lan-wan/where-is-robert-morris-now-.html.

McCool, Grant, and Jonathan Oatis. "Timeline: Big moments in Mueller investigation of Russian meddling in 2016 U.S. election." *Reuters*, March 8, 2019.

Mclaughlin, Jenna, and Donnie O'Sullivan. "Lacking direction from White House, intelligence agencies scramble to protect midterm elections from hackers." CNN. July 27, 2018. https://edition.cnn.com/2018/07/27/politics/agencies-midterms-election-security/index.html.

Meertens, Lambert. "Introduction." *CST Bulletin*, 1983.

Mello, Susan M. "Administering the Antidote to Computer Viruses: A Comment on United States v. Morris." *Rutgers Computer & Tech. LJ* 19 (1993): 259.

Mertelsmann, Olaf, and Aigi Rahi-Tamm. "Cleansing and compromise. The Estonian SSR in 1944-1945." *Cahiers du monde russe. Russie-Empire russe-Union soviétique et États indépendants* 49, nos. 49/2-3 (2008): 319–340.

Middleton, Bruce. *A history of cyber security attacks: 1980 to present*. Auerbach Publications, 2017.

Misa, Thomas J. "Computer security discourse at RAND, SDC, and NSA (1958-1970)." *IEEE Annals of the History of Computing* 38, no. 4 (2016): 12–25.

Modderkolk, Huib. "Dutch agencies provide crucial intel about Russia's interference in US-elections." *de Volkskrant*, January 25, 2018. https://www.volkskrant.nl/wetenschap/dutch-agencies-provide-crucial-intel-about-russia-s-interference-in-us-elections~b4f8111b/?referer=https%3A%2F%2Fwww.google.com%2F.

Mueller III, Robert S. "Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II.(Redacted version of 4/18/2019)," 2019.

Myers, Steven Lee. "Russia Rebukes Estonia for Moving Soviet Statue." *New York Times*, April 27, 2007. Accessed March 1, 2019. https://www.nytimes.com/2007/04/27/world/europe/27cnd-estonia.html.

News, ABC. "World News Tonight." *ABC*, July 8, 1983. https://archive.org/stream/ABCNews19781979/ABC%20News-1983-1984-B-e.txt.

News, BBC. *Russia security paper designates Nato as threat*, December 31, 2015. https://www.bbc.com/news/world-europe-35208636.

Ottis, Rain. "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective." In *Proceedings of the 7th European Conference on Information Warfare*, 163. 2008.

Paller, Allan. "The Five Most Dangerous New Attack Techniques, and What's Coming Next." RSA Conference 2018, 2018.

Parker, Donn B. "How much computer abuse is there?" *COMP. SECURITY J.* 2, no. 1 (1983).

Petersen, Julie K. *The telecommunications illustrated dictionary*. CRC press, 2002.

Quistgaard, Kaitlin. "Yahoo Buys Portal-Puzzle Piece." Wired. 1998. https://www.wired.com/1998/06/yahoo-buys-portal-puzzle-piece/.

"RAND at a Glance." https://www.rand.org/about/glance.html.

Raymond, Mark. "Puncturing the Myth of the Internet as a Commons." *Georgetown Journal of International Affairs*, 2013, 53–64.

Rosenfeld, Seth. *Mario Savio's FBI Odyssey / How the man who challenged 'the machine' got caught in the gears and wheels of J. Edgar Hoover's bureau*. San Franciso Chronicle, October 10, 2004.

Ruus, Kertu. *Cyber War I: Estonia Attacked from Russia*, 2008. https://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia.

Ryan, Andrea, Gunnar Trumbull, and Peter Tufano. "A brief postwar history of US consumer finance." *Business History Review* 85, no. 3 (2011): 461–498.

Sanger, David E. "Utilities Cautioned About Potential for a Cyberattack." *New York Times*, February 29, 2016. https://www.nytimes.com/2016/03/01/us/politics/utilities-cautioned-about-potential-for-a-cyberattack-after-ukraines.html.

Sanger, David E., and Nicole Perlroth. "U.S. Escalates Online Attacks on Russia's Power Grid." *New York Times*, May 15, 2019. https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

Savage, Charlie, Adam Goldman, and Eileen Sullivan. "Julian Assange Arrested in London as U.S. Unseals Hacking Conspiracy." *The New York Times*, April 11, 2019. https://www.nytimes.com/2019/04/11/world/europe/julian-assange-wikileaks-ecuador-embassy.html.

Schmitt, Michael. "Tallinn manual 2.0 on the international law of cyber operations: What it is and isn't." *Just Security*, 2017.

Schneier, Bruce. "About Bruce Schneier." https://www.schneier.com/blog/about/.

Schrager. *Oral history interview with Barry Schrager*. Charles Babbage Institute, 2012.

Schulte, Stephanie Ricker. "'The WarGames Scenario' Regulating Teenagers and Teenaged Technology (1980—1984)." *Television & New Media* 9, no. 6 (2008): 487–513.

Schwartz, Mathew J. "Romanian Hacker 'Guccifer' Extradited to US." Bank Info Security. https://www.bankinfosecurity.com/romanian-hacker-guccifer-extradited-to-us-a-11705.

Scobell, Andrew, David Lai, and Roy Kamphausen. *Chinese Lessons from Other Peoples' Wars*. Technical report. ARMY WAR COLL STRATEGIC STUDIES INST CARLISLE BARRACKS PA, 2011.

Seeley, Donn. "A Tour of the Worm." 1989. http://www.cs.unc.edu/~jeffay/courses/nidsS05/attacks/seely-RTMworm-89.html.

Seligman, Lara. "Pentagon Eyes Windfall as Trump Seeks $750 Billion Defense Budget." *Foreign Policy*, March 10, 2019. https://foreignpolicy.com/2019/03/10/pentagon-eyes-windfall-as-trump-seeks-750-billion-defense-budget-military/.

Shackelford, Scott J, Bruce Schneier, Michael Sulmeyer, Anne Boustead, Ben Buchanan, Amanda N Craig Deckard, Trey Herr, and Jessica Malekos Smith. "Making Democracy Harder to Hack." *U. Mich. JL Reform* 50 (2016): 629.

Simko, Lucy, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. "Computer Security and Privacy for Refugees in the United States." In *2018 IEEE Symposium on Security and Privacy (SP)*, 409–423. IEEE, 2018.

Singer, Peter W. "Military robots and the laws of war." *The New Atlantis*, no. 23 (2009): 25–45.

Smith, Adam. "An inquiry into the nature and causes of the wealth of nations: Volume One." London: printed for W. Strahan; / T. Cadell, 1776., 1776.

Spafford, Eugene H. "The Internet worm program: An analysis." *ACM SIGCOMM Computer Communication Review* 19, no. 1 (1989): 17–57.

———. "Three letters on computer security and society," 1991.

Staff, News. "Dave Weinstein, Former New Jersey CTO, Heads to Private Cybersecurity Firm." Government Technology. 2018. `https://www.govtech.com/workforce/Dave-Weinstein-Former-New-Jersey-CTO-Heads-to-Private-Cybersecurity-Firm.html`.

States., United. *Consumer credit industry: hearings before the Subcommitte on Antitrust and Monolpoly of the Committee on the Judiciary, United States Senate, Ninetieth Congress, first session, pursuant to S. Res. 26.* 3 v. Washington: U.S. Govt. Print. Off., 1967. `//catalog.hathitrust.org/Record/008515191`.

———. *Consumer Credit Protection Act and Truth in Lending Act*. United States. Congress, May 1968.

———. *Social Media Influence in the 2016 US. Election, Hearing Before the Senate Select Committee On Intelligence*. Washington: U.S. Govt. Print. Off., November 1, 2017.

Stiglitz, Joseph E. *Rewriting the rules of the American economy: An agenda for growth and shared prosperity*. WW Norton & Company, 2015.

Stoll, Clifford. "Stalking the wily hacker." *Commun. ACM* 31, no. 5 (1988): 484–497.

Stone, Jeff. "Meet Fancy Bear and Cozy Bear, Russian groups blamed for DNC hack." *Christian Science Monitor*, May 15, 2016. `https://www.csmonitor.com/World/Passcode/2016/0615/Meet-Fancy-Bear-and-Cozy-Bear-Russian-groups-blamed-for-DNC-hack`.

Tabriz, Parisa. "Keynote: Parisa Tabriz." Black Hat USA 2018, 2018.

Tamkin, Emily. "This Is What $1.25 Million Dollars a Month Bought the Russians." *Foreign Policy*, February 16, 2018. https://foreignpolicy.com/2018/02/16/this-is-what-1-25-million-dollars-a-month-bought-the-russians/.

Tasker, Peter S. "Trusted computer systems." In *1981 IEEE Symposium on Security and Privacy*, 99–99. IEEE, 1981.

"The 2nd International Conference on Science of Cyber Security - SciSec 2019." 2019. http://www.sci-cs.net/.

Theisen, Christopher, Nuthan Munaiah, Mahran Al-Zyoud, Jeffrey C Carver, Andrew Meneely, and Laurie Williams. "Attack surface definitions: A systematic literature review." *Information and Software Technology* 104 (2018): 94–103.

Thomas, Moore. *Utopia, 1516*, 1965.

Tikk, Eneken, Kadri Kaska, and Liis Vihul. *International cyber incidents: Legal considerations*. Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010.

Hackers found guilty of selling computer codes, 1990.

Times, New York. *British Finance Companies Map Credit Ratings for Consumers*, November 29, 1960.

———. *Paperback Best Sellers*, February 10, 991. https://timesmachine.nytimes.com/timesmachine/1991/02/10/949391.html.

———. *Senate Investigators Examining Reports of Faulty Credit Ratings*, May 23, 1968.

Timm, Trevor. "It's time to stop using the "fire in a crowded theater" quote." *Atlantic* 2 (2012).

Tuchman, Barbara Wertheim. *The Guns of August*. Macmillan, 1962.

Tuma, Katja, Gül Çalikli, and Riccardo Scandariato. "Threat analysis of software systems: A systematic literature review." *Journal of Systems and Software* 144 (2018): 275–294.

Uzunov, Anton V, and Eduardo B Fernandez. "An extensible pattern-based library and taxonomy of security threats for distributed systems." *Computer Standards & Interfaces* 36, no. 4 (2014): 734–747.

Vieira, Barbara. "Is software security improving?" *ABN AMRO*, January 24, 2019.

Ware, Willis H. *Oral history interview with Willis Ware*. Charles Babbage Institute, September 2003.

Ware, Willis H. *Security controls for computer systems*. Technical report. RAND CORP SANTA MONICA CA, 1970.

Waterfield, Bruno. "Ban Koran like Mein Kampf, says Dutch MP." *The Telegraph*, 2007. https://www.telegraph.co.uk/news/worldnews/1559877/Ban-Koran-like-Mein-Kampf-says-Dutch-MP.html.

Watson, Nigel. *An abridged version of the Experian: the story so far*. Experian Inc. 2013.

Weiner, Rachel, and Spencer S. Hsu. "Hacker known as Guccifer sentenced to 52 months in prison." Washington Post. September 1, 2016. https://www.washingtonpost.com/local/public-safety/guccifer-hacker-who-revealed-clintons-use-of-a-private-email-address-sentenced-to-52-months/2016/09/01/4f42dc62-6f91-11e6-8365-b19e428a975e_story.html?utm_term=.fe28ecdcb503.

Wilkinson, Claire. "The Copenhagen School on tour in Kyrgyzstan: Is securitization theory useable outside Europe?" *Security dialogue* 38, no. 1 (2007): 5–25.

Wu, Chris. "An Overview of the Research and Development of Information Warfare in China." In *Cyberwar, Netwar and the Revolution in Military Affairs*, 173–195. Springer, 2006.

Xu, Shouhuai. "Cybersecurity Dynamics: A Foundation for the Science of Cyber Security." http://www.cs.utsa.edu/~shxu/socs/.

———. "Emergent behavior in cybersecurity." *arXiv preprint arXiv:1502.05102*, 2015.

———. "Homepage." http://www.cs.utsa.edu/~shxu/.

Yagoda, Ben. "How Old Is 'Gaslighting'?" *The Chronicle*, January 12, 2017. https://www.chronicle.com/blogs/linguafranca/2017/01/12/how-old-is-gaslight/.

Yost, Jeffrey R. "The Origin and early history of the Computer Security Software products industry." *IEEE Annals of the History of Computing* 37, no. 2 (2015): 46–58.

Zengerle, Patricia, and Emily Stephonson. "Trump says he will accept election result - if he wins." *Reuters*, October 19, 2016. https://www.reuters.com/article/us-usa-election/trump-says-he-will-accept-election-result-if-he-wins-idUSKCN12J0ZM.

Zhang, Lena L. "Behind the 'Great Firewall' Decoding China's Internet Media Policies from the Inside." *Convergence* 12, no. 3 (2006): 271–291.