CENTRE FOR COMPARATIVE STUDIES OF CIVILISATIONS
JAGIELLONIAN UNIVERSITY IN KRAKÓW

The Polish Journal of the Arts and Culture. New Series 7 (1/2018): 7–28 [ARTICLE]
DOI: 10.4467/24506249PJ.18.001.9775

Cyberthreats in Popular Visual Culture

Myriam DUNN CAVELTY, Lorretta HOLLOWAY

Abstract

This paper focuses on how cyberthreats have been represented in popular visual culture (Western and Asian). These cultural products are an interesting site where the technical and the political effects of cyberthreats are presented together, giving them a particular weight and place in the discourse. The paper discusses three dominant representations (machine out-of-control, computers used as weapons, and amassing or withholding of data as threat) and then identifies three commonalities between them. The first concerns the surprising "passivity" of technology, making the human the main problem in this story, the second is the importance of non-virtual geography, turning machines into mere additions of normal human life, and the third concerns the normalization of the threat through time. Cyberthreats are part of our lives now and they are so deeply embedded, they cannot be separated from them anymore.

Keywords: *cybersecurity; cyberthreats; popular visual culture; security politics; visual studies; visuality*

Myriam DUNN CAVELTY, security studies scholar, senior lecturer and deputy head of research and teaching at the Center for Security Studies at ETH Zurich, Switzerland. Her research interests include the politics of risk and uncertainty in security politics and changing conceptions of (inter-) national security due to cyber issues in specific.
E-MAIL: dunn@sipo.gess.ethz.ch

Lorretta HOLLOWAY, Vice President of Enrollment and Student Development Framingham State University, USA. Her research interests include cross-national standards for college and career readiness and emergency preparedness. Before becoming an administrator, she was a professor in the English Department at Framingham State University for 15 years.
E-MAIL: lholloway@framingham.edu

1 Introduction

The frictionless operation of digital technologies has become an essential foundation for prospering economies and stable societies today. As a result, threat discourses focusing on cyberincidents, understood as disruptions of these routine operations, have come to hold a prominent position in society. An analytically noteworthy but previously underappreciated fact about cyberthreats is that they remain invisible until they manifest as cyber*incidents* and deliver effects.[1] They become visible – and therefore perceptible and ultimately politically actionable – *only* through their performance and by extension their effects in the technical sphere but also the social and political realm.

But what do cyberthreats – broadly understood – even look like? There are a few options for their visualization; once a cyberincident has occurred, there is a possibility to isolate the code of the malware that caused it through reverse engineering. The cyberthreat then looks like programming language. In addition, cyberthreat could also have a face – the face of a well-known hacker like Gary McKinnon (aka Solo) for example[2]. However, this is not the type of visuality we are interested in. Code per se does not represent danger. The individual faces of famous hackers reveal "normal guys" next door, some of them over 50 years old. Both types of visuals only convey a threat because the code or the person depicted has already created a negative effect, one that has been categorized according to known cyberthreat categories or fixed legal principles.

In this article, we are interested in how such categorizations become possible in the first place – the space in which the recognition and categorization of danger is shaped. While there are plenty of publications on the potential effects of cyberthreats and on solutions against them in all kinds of disciplines[3], there are none on how visuals influence perceptions of such threats by the public. We can begin to fix this by turning towards visual representations of cyberthreats, the most pertinent and spectacular of which are found in popular visual culture such as films and TV shows. As Lee Clarke argues,

[1] T. Balzacq and M. Dunn Cavelty, *A theory of actor-network for cybersecurity*, pp. 176–198; also J. Parikka, *Ethologies of Software Art: What Can a Digital Body of Code Do.*

[2] Among other things, the Scottish national hacked into more than 97 US military and NASA computers in 2002, making them useless for 24 hours while he searched for evidence of extra-terrestrials.

[3] M. Dunn Cavelty, *Cybersecurity Research Meets Science and Technology Studies*, pp. 22–30.

imagination, rather than calculation, underpins our understanding of threats.[4] Of all possible representations, visual media is the only place that gives us spectacular visuals for cyberthreat scenarios; therefore, they reveal aspects of politics "that are hardly graspable without attention to the visual"[5].

The article has three parts. In the first part, we outline our theoretical and practical approach. In the second, using a mix of discourse analysis and semiology, the default method in most visual studies[6], we study a variety of films and TV series for representation of cyberthreats. We attempt to broaden the discussion of cyberthreats beyond just Western representations and include popular visual culture from the East. We conclude with reflections on what we found, pointing to the normalization of this type of threat – and what it signifies for society.

2 The Approach

One on the most influential theories from the field of critical security studies is the so-called "securitization theory", a combination of writings based on the first generation of the Copenhagen School[7] plus later iterations that added a stronger sociological focus[8]. What these publications have in common is an interest in how threats are constructed in political processes and what the political and social consequences of these constructions are. Security, so the literature says, is entrenched in symbolic and cultural contexts, which generate meanings for actors and audiences through relational dynamics. Lene Hansen, who has most prominently theorized the role of images in securitization processes[9], writes that even though images are undoubtedly

[4] L. Clarke, *Worst Cases: Terror and Catastrophe in the Popular Imagination*, p. x.

[5] R. S. Andersen, J. Vuori, and C. E. Mutlu, *Visuality*, p. 94.

[6] G. Rose, *Visual Methodologies: An Introduction to Researching with Visual Materials*, p. 188.

[7] B. Buzan, O. Wæver, O. and J. de Wilde, *Security: A New Framework for Analysis.*

[8] T. Balzacq, *The Three Faces of Securitization: Political Agency, Audience and Context*, pp. 171–201; J. Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU*; H. Stritzel, *Towards a Theory of Securitization: Copenhagen and Beyond*, pp. 357–383; M. Salter, *Securitization and desecuritization: a dramaturgical analysis of the Canadian Air Transport Security Authority*, pp. 321–349; *A. Neal, Securitization and Risk at the EU Border: The Origins of FRONTEX*, pp. 333–356.

[9] L. Hansen, *Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis*, pp. 51–74; also: L. Hansen, *How images make world politics: International icons and the case of Abu Ghraib*, pp. 263–288.

important and need special attention, they do not have the power to securitize anything by themselves. Rather, pictures depend "upon someone or somebody – a securitizing actor – who holds that the image demonstrates a threat-defense urgency and calls for an immediate response"[10].

In a similar vein, we claim here that popular visual culture works its securitizing power through that "symbolic and cultural context". Given that pop cultural products are a "temporary embodiment of social processes that continually construct and deconstruct the world"[11], analysing them helps us understand this symbolic and cultural context fairly well. In contrast to other forms of expression, visual art is known to more directly create affective intensities[12] and to lend itself exceptionally well to the production and circulation of emotions. That makes such visuals powerful in security politics, which at least in large part relates to emotions such as hate and fear.[13]

We argue that if an issue has not yet been securitized and the audience therefore needs to be convinced of the urgency of the threat, visual narratives can serve as powerful mobilizers either directly or indirectly and can legitimate and validate the security discourse.[14] If the audience is already convinced of the threat, it expects that securitizing actors continue to maintain the securitized environment in accordance to how the dominant threat has been framed.[15] In this case, popular visual culture serves as reminder and enforcer of which issues are existential threats and thus require policy reactions.

The symbolic and cultural context that contains threat representations is highly fluid and dynamic. First, it is constantly enriched with new knowledge about threats based on various types of reports ranging from media representations to expert opinions on past incidents but also on other forms of representations including literature and film. Importantly then, this context contains knowledge about past incidents as well as knowledge gained from fictional representations of the threat.[16] What we are looking at is a

[10] L. Hansen, *Theorizing the image for Security Studies: Visual securitization and the Muhammad Cartoon Crisis*, p. 53.

[11] T. Cresswell and D. Dixon, *Introduction: Engaging Film*, p. 1. See also: J. Weldes, *Going Cultural: Star Trek, State Action, and Popular Culture*, pp. 117–134.

[12] B. Massumi, *From Parables for the Virtual: Movement, Affect, Sensation.*

[13] R. Bleiker, *Aesthetics and World Politics.*

[14] F. Möller, Photographic Interventions in Post-9/11 Security Policy, 179–196; I. Neumann and D. Nexon, *Harry Potter and International Relations,* pp. 17–20.

[15] B. Buzan, O. Wæver, O. and J. de Wilde, *Security: A New Framework for Analysis*, p. 27.

[16] T. Carver, *Cinematic Ontologies and Viewer Epistemologies: Knowing International Politics as Moving Images*, p. 426.

"hybrid reality" that goes beyond "what has been" and creates meaning for threats that "might be". At the same time, this knowledge flows out into society through the various channels mentioned above and can be deliberately tapped into by political actors if the need for interpretation arises.

Our focus on aspects of visual popular culture is further justified because the majority of studies on cyberthreats and their political representations have to date used written material as data, consisting of elite produced speeches or official reports.[17] This literature generates insights into how security-meanings are constructed through the connection of the "cyber" prefix to well-known threat categories and how concepts such as "cyberwar", "cyberterror", or "cybercrime" generate specific political effect. However, it fails to address how these categories are made palpable by specific visual threat representations in the symbolic and cultural context of threat-making that provide a framework for interpretation when incidents become visible and generate effect. "Reading" popular visual culture will allow us to see one facet of how a shared understanding of cyberincidents is forged through visual representations of an otherwise invisible threat.

We focus on representation of cyberthreats in films and TV series over time and in Western and in Asian entertainment products. Using a set of keywords related to cyberthreats and hacking[18] to identify the relevant products through the Internet Movie Database (IMDB), we compiled a list of products to study (see Appendix 1). They are scattered through time, which allows us to look for change over the years and come from Eastern and Western cultures, which allows us a more diverse picture that may differ from only Western threat imaginations.

3 The Analysis

Our analysis reveals three representations of cyberthreats.[19] We discuss them below in what we call "clusters". In the first cluster, the main threat is a

[17] L. Hansen and H. Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, pp. 1155–75.

[18] These keywords are: cyberthreats, hacking, hacker, cyberwar, cyberterror, cybercrime, computer threat, and other combinations.

[19] A note on how representative the list is: Once we identified the three clusters, we checked other possible movies and series to see whether they would deviate from our findings. Since this was not the case, we believe the three threat representations are robust.

machine, mechanical and mobile or a computer with software, that is "out-of-control" and threatens human existence. In the second, computers are weapons, with which physical objects can be blown up. In the third, single machines have lost importance; instead, the data stored on increasingly networked systems and the power structures this data supports matters the most. The threat emanates from corrupt power structures or organizations that possess data that they keep secret or use to manipulate people. Interestingly, Asian cyberthreat representation is predominantly situated in this third cluster.

3.1 The Intelligent-Malicious Mainframe

This trope is related to artificial intelligence and machines out-of-control. In *Tron* (1982), the main "villain" is the Master Control Program or MCP, an artificial intelligence entity inside the mainframe of a large business entity. When it tires of its responsibilities, it plans on seizing control of the entire US. It states that it "could run things 900–1200 times better than any human". Visually, it is shown as large, black desk touch screen, which has a mechanical voice and later resembles a giant, spinning, vicious red demon head in the virtual realm.

In the movie *War Games* (1983), a super-computer called WOPR (War Operation Plan Response) nicknamed "Joshua" after his creator's dead son is a computer responsible for all nuclear missiles in the United States. It is a game computer, programmed to repeat strategic simulations to learn from its mistakes. A curious teenager hacks into this computer and accidentally starts a game of Global Thermonuclear War. In what follows, the computer continuously feeds false data, pushing NORAD into raising the DEFCON level toward a "retaliation" that would have started World War III. Joshua is a large, clunky computer, which has a row of lights to signify activity. Crucially, it too has a voice to communicate, which is understandably very common in all of the movies that depict computers as protagonists.

In *Ghost in the Shell* (1995), the mysterious hacker known as the Puppet Master is a sentient program, initially written as a highly secret hacking program by a secret government organization; however, and in a special twist distinguishing this movie from all the others, he turns out to be truly benign and simply interested in experiencing mortality.

In the *Matrix Trilogy* (1999–2003), highly advanced machines are the dominant civilization after they rebelled against humanity and imprisoned

most of them in a neural-interactive virtual world known as the Matrix. They may be a distributed system of individual entities, but the "Deus Ex Machina" ultimately controls them. It has the face of a human, formed by thousands of tiny, insect-like machines. In the same series, there are "sentient programs" inside the simulation ("agents") that can move in and out of everyone. Like every program, they are built on a specific set of rules. However, Agent Smith, visually resembling the cliché image of a secret agent goes "rogue" and becomes a threat to the entire system by infecting everything as a virus, which is ultimately what makes peace between machines and humans possible.

Interestingly, the threat these machines and programs create is in all cases directly related to human action and decisions. In *Tron*, the rogue program starts out as only a chess program but is later substantially modified by a power-hungry and morally corrupt CEO in order to administer the company's computer network and hide his dirty secrets. In *War Games*, Joshua is installed because humans are judged to be too slow and too emotional when it comes to launching nuclear missiles. Because it is a not-so-intelligent machine after all, it cannot distinguish between reality and fiction – everything is a game to him that he has to finish playing. That the teenage hacker is able to break into this machine in the first place is the fault of its creator, who left a virtual backdoor open and made guessing the password relatively easy. In *Matrix*, the machines are peaceful entities – with their own nation – before the humans try to destroy them by "scorching the sky" with nuclear weapons due to their dependency on solar energy.

While a common topic in all these representations rests on the computational incapacity for compassion and emotion and the distinct "otherness" of the machines visually, even though they are given human features in all instances, the human fault and judgment errors causes the cyberthreat.[20] The common wish to delegate activities to machines because they are ultimately "better" at such activities backfires because the machines start performing in ways that are detrimental to human interests. We then need the "hacker" to physically stop them. In *Tron*, it is a hacker who "enters" the machine world. In *War Games*, the same teenager who set in action the game "outsmarts" the machine by having it play a simple game of Tic-Tac-Toe, a futile game

[20] One of the peer reviewers shared an interesting thought here that we think should not be lost to the readers: "This trope somewhat inverts one of the Christian theological dilemma permeating Western pop culture: whether it is god-pancreator who is ultimately responsible for the evils caused by humans. Here, humans create a superhuman of a kind (powerful, wise, etc.), who himself is a child-deity mixture."

between two experienced players because it also ends in a stalemate, which makes the machine realize that the "game" Global Thermonuclear War is a no-win game in which "the only winning move is not to play". *The Matrix* depicts the super-hacker Neo as a Jesus-like saviour who manages to negotiate a peace treaty between machines and humans through a deal with the Deus Ex Machina.

These heroes use "war-dialing", which signifies the use of a modem to automatically scan a list of telephone numbers[21], and "hacking" to control these computers. However, not surprisingly, the physical-material aspects of this struggle are more dominant in the visual media. In *Tron*, the MCP digitizes a programmer, who then allies with a security program inside the machine world in which programs have human form and human emotions – but ultimately blows the red demon head up, which equals the deletion of the program. In *War Games*, the ultimate threat is global nuclear war, which is shown through inside views of a silo in which a nuclear missile gets ready to launch. The computer Joshua is a very large physical entity in the Cheyenne Mountain Complex, an actual military bunker in Colorado Springs. Large parts of the movie play inside that bunker and next to Joshua, who physically struggles through frantic lights, smoke, and explosions to solve the puzzles given to him. The *Matrix* may play with the categories "real" and "virtual" more than other movies, but it, too, places the main struggle in the "real" world and not in the simulation. The machines in the real world are defeated only with electromagnetic pulse weapons. Neo's physical presence within the Machine City and ultimately his physical death is needed to end the war.

There are two kinds of powers revealed in this trope. One kind is the power over life and death. These machines "out-of-control" are a threat to human life, often on a global scale. The other sort of power rests in the hands of specific and especially talented individuals. They have a kind of technical super-power and have become part of the hacker "myth"[22] that was in part co-shaped by movies such as *War Games*. Because machines are the prime threat in this trope, these individuals are not. In fact, they become heroes because they ensure that humanity prevails over the threat that machines pose.

[21] The movie *War Games* gave this hacker technique its name. Previously to *War Games*, it was called "hammer dialing" or "demon dialing." More proof of the influence of visual representation on field.

[22] R. Skibell, *The Myth of the Computer Hacker*.

3.2 Computers as Weapons

However, when we think of how large-scale cyberthreats are talked about in the mainstream media, we are increasingly presented with hacking turned weapon rather than some fight between a cold machine and noble, warm-hearted man. The humans in these cases are malicious actors with no noble intent whatsoever or who may have started with a noble intent but were frustrated in their good goals. *Die Hard 4* and *Blackhat*, on which we will mainly focus below, and to some extend *Skyfall*, but also many TV show episodes[23] include this plot device. The targets of cyberattacks in these movies and TV shows are so-called critical infrastructures or utilities, an extension of modern societies. This way, spectacular disaster scenarios are possible – disaster scenarios that have populated the "real world" cyberdiscourse since the latter 1990s.

The plot in *Die Hard* is based on article called "Farewell to arms"[24], a long-form journalistic article featured in Wired Magazine.[25] The article, which is mentioned in the opening credits of the film, pertains to the future and changing landscape of information warfare in the digital age and argues that the perceived convenience of digital connectivity comes at the cost of potential insecurity. That is the premise of the movie. It shows a three-stage systematic attack on critical infrastructure – transport systems, financial systems, public utilities like electricity, gas, telecommunication – almost causing the collapse of the American society. Anything that's run by computers all down at once reflects real concerns of emergency management planners.[26]

The main villain, Thomas Gabriel, is called a "cyberterrorist", but he is also an insider turned disgruntled employee. A former chief programmer for America's infrastructure security in the Department of Defence, Gabriel

[23] See shows like *Le Femme Nikita*, *Pied Piper*, *Bloody Monday* Season 2, Season 9 of *24*, *Cybergeddon* etc.

[24] J. Carlin, *A Farewell to Arms*.

[25] In that same year, the Presidential Commission on Critical Infrastructure Protection published their seminal report, in which the link between critical infrastructures and cyberspace was established in the political realm: President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures*.

[26] For example, infrastructure systems—power, water, sewer, transportation, and communication—in many countries all depend upon computers working properly. These areas are listed as primary places of attention in the *Executive Handbook for All-Hazards Preparedness* co-published by the U.S. Department of Homeland Security and the Federal Emergency Management Agency. January 2017.

hacked into and shut down the North American Aerospace Defence Command (NORAD) with a laptop to prove how vulnerable America was to a cyberattack. When he tried to go public with his knowledge after being threatened, the government publically humiliated him and dismissed him. He and his group of skilled hackers start the fire sale (it's called this because "everything must go") on the day before 4th of July and send a message made up of clips from various presidents across the country to create fear. Subsequently, he and the others travel around Washington D.C. in a trailer pulled by an eighteen-wheeler to keep from being located and hack everything they get access to. The hacks are extremely effective. Cars crash all over the US when the hackers meddle with the traffic systems. Mass panic ensues after a fake explosion of the US Capitol building is shown on every TV screen across the country. They manipulate the anthrax alarm system in the FBI building to have everyone evacuate. Gabriel kills people by blowing up their computers from a remote location, and he blows up a gas station by redirecting all the gas in the system to it. The devastation occurs not because of computers but because of our reliance on computers and the ease with which this reliance is manipulated. Usually, this ease of manipulation makes our lives better, even safer. However, in the wrong hands, the ease has disastrous consequences.

In *Blackhat,* the protagonists use malware that is based on the famous Stuxnet attack[27], and the major hack that the characters are trying to prevent is targeted at critical infrastructure as well. Targets include an atomic power plant, the financial system, and rare mineral site. As in *Die Hard 4*, in *Blackhat*, we once again have hackers going against other hackers in a kind of duel, but this time as a central plot-point. Government entities are powerless against the threat. They try hard, but they do not have the necessary skills or are bound by rules that restrict them. The hackers they recruit to help them on the other hand can and do bend the rules where necessary. In both movies, these hackers need to move around physically. *Blackhat* has locations in many different countries, including Indonesia and China, and they also need to get their hands dirty to end the threat, with lots of guns and lots of explosions. Given the need for spectacular images in movie blockbusters (especially the *Die Hard* franchise's particular brand) this is no surprise; however, it also creates a very particular type of public impression of

[27] M. J. Gross, *Stuxnet Worm: A Declaration of CyberWar*. It is also shown in *Person of Interest* S04E5.

cyberthreats. Given the vulnerabilities of infrastructure systems and given the extreme impacts, cybertools become depicted as weapons as effective as guns and explosives.

Directors visualize these threats by presenting fast typing fingers on keyboards, by having code speeding by on screens to show that a program is being executed, or with visuals related to explosions in machinery or factories or cities. On film, computers are manipulated like magic and code is translated into meaning by visually appealing pictures on screen that show 3D building plans or gas flowing in pipelines or how traffic is currently routed (*Die Hard*). Infection by malware is represented by light flowing along cables and computer hardware. When it has reached a target, a light goes on – it is now rigged, armed, and ready to go up in flames (*Blackhat*).

These images have become the go-to images for these situations in the way a shot of clock with the hands speeding along or a calendar with pages blowing off in films of the 30s and 40s came to symbolize fast forwarding in time. Now film depicts the net as an extension of and a connection between physical objects, which have fixed locations. They show our vulnerability through the ability of being able to reach so many of these systems through a computer connection from anywhere in the world.

This vulnerability makes a double-appearance in this trope. On the one hand, malicious actors for malicious deeds exploit it. On the other, it leads to a fundamental distrust of digital technologies by those with special knowledge. The hackers in *Die Hard 4* all have redundant systems for communication in case the information infrastructure breaks down. The main good hacker in *Blackhat* tells his FBI handler that he has learned that any digitally stolen money can be made "real" by getting money out in cash from different cash machines and walking away. Both McClane, the main protagonist in the *Die Hard* movies, as well as Bond in *Golden Eye* and *Skyfall* represent the "old" world, where things are done the "old" ways and not with the help of computers. McClane shouts at his hacker-helper: "It's not a system. It's a country – you are talking about people"! The new world almost manages to throw Bond and all he stands for ("We're a bunch of antiquated bloody idiots, fighting a war we don't understand and can't possibly win") into a deep identity crisis in *Skyfall* – but what counts in the end is the gritty reality of the battlefield, where true heroes fight face-to-face and purpose and meaning can be restored.

How the global aspect of cyberspace is shown or not differs considerably. *Blackhat* and the Bond movies take great care to move their protagonists

around the globe when tracking down the villains. The threat scenario is a global one in *Blackhat* – the cyberterrorist uses the entire world to stage his scheme and attacks targets in different countries. In *Die Hard 4*, the stage is Washington DC and the end of the world is about to go down in the American Capitol. Global or local, what these movies have in common is the ways the "threat" is identified: visually. Gabriel is identified by McClane with the help of a video-call, which allows the FBI to recognize him immediately and also know his intent exactly (*Die Hard 4*). Surveillance cameras play a role throughout the movie to provide visuals for friend and foe and the audience. In *Skyfall*, Bond tracks down the villain and they meet face-to-face. In *Blackhat*, surveillance cameras are used again to track villains. Hiding ones identity and hiding one's location is ultimately futile.

3.3 Secrets, Power, Resistance

This new world order of not being able to hide from computer knowledge about us or its affect on our personal lives has become common place. It raises questions about the idea of personal security in cyberspace by making the viewer wonder from whom or from what we really need to be protected. While the enemy in the first two tropes are made plain nearly from the beginning, this next section focuses on how people in power use trappings of cybersecurity to control information. This trope defines the films *The Net* (1995), *Johnny Mnemonic* (1995), *Prophecy* (2015) and to some lesser degree the two Bond movies with hacking elements, *Golden Eye* (1995) and *Skyfall* (2012). The trope is also at the centre of the battles between the "good guy" hackers and the "bad guy" hackers in televisions dramas. The threat in this trope is ultimately not the hacker or the machine, but the entities that amass information about individuals and use that information for their own gain. It is not computers or machines that emerge as the main threat, but human organizations or human individuals. Though these threats could lead to large-scale disasters, most of these villains work on a personal level of concern.

Often in this subgenre, we encounter the use Hitchcock's favourite character – the Innocent Person Wrongly Accused – to dismantle and ultimately destroy evil power structures at great personal cost. In *The Net*, a female computer security specialist stumbles across a sinister network of cyberanarchists that are pulling a large-scale computer scam that consists of selling a security program, which is actually just a big backdoor that gives its pro-

grammers access to pretty much everything. In *Johnny Mnemonic*, technology overload causes NAS (short for nerve attenuation syndrome) in large parts of the population. A multination company named PharmaKom keeps the cure for NAS a secret because selling drugs to remedy the disease is more profitable than curing it; however, an underground resistance movement steals it and hires a data courier to reveal this information to the broader public. The computer security specialist and the courier merely do their jobs but get caught up in a bigger fight that makes the threat to their own personal autonomy a snapshot of what seems to be occurring to society as a whole, perhaps even without our knowledge.

Such parallel constructs occur in the Japanese drama *Bloody Monday* in both seasons (2008, 2010). Based on a manga of the same name, the drama depicts a world where a seemingly regular high school student turns out to be a highly trained genius hacker bullied into working for the government to counter a cult that wants to release a virus in Tokyo. As both seasons unfold, viewers realize that the Biology teacher at the school is a hired killer and one of the people near our hero is actually a cult member. What seems on the surface an ordinary world with ordinary people hides another world where the lives and deaths of millions are in the hands of a few hackers who fight each other online and offline.

Despite the continued popularity of depicting such large-scale threats in film and television, cybersecurity, with the increasing common use of the internet and the use of social media, is becoming more personal. *The Net* from 1995 is one of the first movies that depicts the internet as the system we know nowadays. It emerges as a blessing and as a curse at the same time; it is a place where we can order pizza and get it home delivered, but it is also a place where we leave digital traces that make us more visible in a space that perpetuates insecurity. One of the famous and at the time prophetic comments of the main character is the following:

> They knew, they knew everything about me. They knew. They knew what I ate, they knew what I drank, they knew what movies that I watch, they knew where I was from, they knew what cigarettes I used to smoke, and everything they did, they must have watched on the Internet, watched my credit cards. Our whole lives are on the computer.

Truth seeking, not surprisingly, becomes an underlying focus for many of the dramas where there is more time to delve into character and their

individual needs for truth. If this truth lies in multiple layers of computer data files, then anyone with any cybersecurity experience will become a key player in moving plots along. One of the most famous hackers in Asian dramas is Hacker Ahjumma from the South Korean drama *Healer* (2014–2015). She is a secondary character but ironically the character to whom our title character is the closest, at least before he meets the love interest in this story. She not only manages all his jobs, but also provides all his emotional and tech support. So while he is the one in physical danger, she is the one who provides him an electronic road map for his jobs and also the means for him to find information. Her character represents a trend of "good" hacker as necessary co-pilot for the lead who has to physically fight in the "real" world that the hacker helps manipulate.

Healer represents an increasing trend in dramas that include groups of people who band together to rebel against the monopoly and manipulation of information by larger entities. While *Bloody Monday* also has a group supporting the lead, they are fighting together for large-scale security – plague-like disease, nuclear disaster. However, with the increasing concern about personal information leaks and manipulation in the cybersecurity world,[28] it should come as no surprise that these newer hackers do not necessarily focus on corporate secrets but the lives of individuals. Thus, we also increasingly see the personal pain of the individuals in these groups caused by the manipulations by some larger conglomerate.

In *Lookout* (South Korea), the team consists of members who each suffered through a tragedy that has been covered up by the authorities for the comfort and gain of the wealthy. There is a hacker who lost his mother, and a young woman who is so afraid to leave her house since her whole family was murdered, who only follows the world through security cameras. The members of the Special Invesitgations Unit in the Japanese drama *Crisis*, including a female hacker, have all been selected because they were in trouble before, but the government needs their skills to protect officials. However, while they do these jobs, they begin to question the morality of the system they serve, especially when the deaths mount. In *Mr. Robot* (premiering in 2015) E-Corp – or Evil Corp, as the main protagonist likes to call them – is one of the largest multi-national conglomerates in the world, and the main protagonist thinks they are responsible for his father's death. He joins a hacktivist

[28] See growing interest (and profitability) in companies like Lifelock at Lifelock.com. These companies claim, for a fee, to protect their clients from cyber identity theft.

group, which wants to cancel all consumer debt by destroying the data of that company.

Japan's *Final Cut* (2018) represents a contemporary form of manipulations of social media for justice and revenge. Keisuke Nakamura, the protagonist, utilizes his friend and partner's cybersecurity expertise – which does not just include hacking, but hidden cameras, and video manipulation – to make money by being avenging angels for people who complain about unfair treatment on social media. However, his ultimate goal is to clear his unfairly convicted mother's name. The drama focuses on how he uses the information about each person involved in the case – all personal data found through security breaches online and in person – to create videos for blackmail and retell the story that was manipulated long ago through the internet.

Thus in this trope, possessing information is power, but stealing this information and spreading or deleting it also is a form of power – and resistance. In the larger context of this, hacker-resistance, depending on how the set-up of "good" and "bad" is framed, can also emerge as the main threat to state entities, while at the same time raising crucial questions of right and wrong. Cybervigilantism as a form of resistance is central in *Prophecy* (Japan, 2015), *Pied Piper* (South Korea, 2016), *Crisis* (2017), *Lookout* (2017), and *Final Cut* (2018). Tragic anti-heroes violently fight what they consider injustices in society, standing up for "bottom earners", the bullied and the outcasts (*Prophecy*, *Lookout*, and *Final Cut*) and/or fighting corrupt conglomerates with ties to politics (*Pied Piper, Lookout, Crisis, and Final Cut*). Using social media to gain attention and to morally educate netizens, they fight for something that we recognize as noble despite the fact that we cannot fully agree with their methods without feeling morally uncomfortable. To the special police units hunting them, the cyberthreat manifesting through the actions of these individuals or groups causes social unrest, panic, and use of violence against targets of their campaigns.

In contrast to the first two clusters, the threat in this third one is much more diverse. The referent object is, too; it sometimes is "the truth" that needs special protection and care (*The Net*, *Johnny Mnemonic*, *Prophecy*, *Pied Piper*, *Mr. Robot*, *Crisis*, *Lookout*, *Final Cut*) and sometimes it is "the secret" (*Golden Eye*, *Skyfall*). Deliberate cyberincidents through hacking become a tool to attain specific goals. Given the centrality of "data" in this trope, data storage devices become visually and narratively important: floppy disks with sensitive information (*The Net),* fancy launch disks *(Golden Eye*), flashdrives (Final

Cut, Lookout), hardware drives containing details of undercover agents (*Skyfall*, *Pied Piper*, *Crisis*), or brain implants to carry encrypted data from one place to another (*Johnny Mnemonic*). Thus the visual becomes physical but also portable. Unlike the giant computers in the first trope, these can be seen as more dangerous because they could be and are "carried" by anyone anywhere right under our noses just like the computers we carry around with us each day.

4 Conclusion

In this paper, we have looked at how cyberthreats are visualized in popular visual culture since the early 1980s. The multifaceted visualizations of cyberthreats are part of the symbolic and cultural context in which security-related meanings and practices are embedded. In contrast to existing studies on cyberthreat representations, this visual element pays particular attention to how cyberincidents deliver effects and can add to our understanding of affective elements in threat representation.

By familiarizing and normalizing particular ways of seeing cyberthreats, popular visual culture feeds into a reservoir of knowledge containing a "mixed reality". This is not to say that people are unable to differentiate between fact and fiction. However, the close cross-fertilization of fiction and reality invites an additional reading across all three threat representations to identify common, potentially not easily apparent, maybe even surprising aspects of this mixed reality. Three such commonalities seem particularly noteworthy: one concerning the surprising "passivity" of technology, the second being about the importance of non-virtual geography, and the third about the normalization of the threat through time.

The first observation is about the portrayal of technology across all threat representations. Popular visual culture places the blame for cyber-threats squarely on the shoulders of humans in stark contrast to what is known as "technological determinism" – the assumption that technology determines the development of a society's social structure and cultural values. Even when machines come to life and develop their own "intelligence" and agency, the arising threat is ultimately a result of human failing. Across all the cultural products viewed, technology is shown as a mere amplifier of negative human character traits and an enabler for extending moral shortcomings through virtual space into other localities. It makes cybersecurity an issue of

moral conduct, propagating intervention strategies targeting human conduct rather than technologies.

The second observation concerns the relationship between virtual and non-virtual space. In the real-world, the borderless nature of virtual space has often been called a problem, since hiding from the law becomes easy and it is making it particularly hard for nation states to react to the threat with the traditional legal tools based on the notion of sovereignty. In contrast, in popular visual culture, it is always the real world in which security and insecurity unfolds and there is no anonymity. The threat is real with real impact: well-known violence that can be countered with equally violent means. Consequently, the threat, machine or human, can also be localized and tackled. This echoes some of the more recent debates in the real-world. Since the cyber-domain is not a natural environment that develops beyond human control but is in fact built and regulated by humans, it is almost entirely malleable. In other words, traditional response strategies and rules of conduct can be made to apply – at least in part. Thus, despite the fact that the threat is severe and pervasive, grounding it in the corporeal world makes it manageable with well-known security strategies.

A third observation concerns the "normalization" of the threat over time. Computers and their abilities are portrayed as exceptional or spectacular in the early years, but as we move through time, the "cybered" aspects of society become an everyday feature of life. With the delegation of not only a few but more and more tasks to machines, cyber-threats become a normal, systemic, even anticipated condition. As expected, with this normalization comes advanced familiarity with the threat in society, both in fiction and reality. In the entertainment industry, the attention given to "hackuracy" has massively increased over the years.

Why there is a need for more accuracy is pure speculation, but maybe it is because cyberthreats have become much more deeply embedded into our daily lives. With the increased frequency with which we hear about incidents comes a kind of "normalization". With the ability to find so much information about people online without much hacking expertise – see all the cases of doxing we have going on through use of social media, the posting false reports about people that go viral, the posting of personal information about one's "enemies" so your followers can launch a protest or attack, identity theft – it shouldn't surprise us that dramas show an increasing normalization of the use of the cyberdimension as a place to take revenge or get

vigilante justice when the official system is or appears to be broken. With all the email phishing scams in our places of employment and the attacks on systems,[29] cyberthreats are part of our lives now, and even though they still often remain spectacular and surprising, there is a certain, eerie familiarity to them.

[29] For example, in September of 2018 the United States Department of Education sent out a warning nationally that students on financial aid were being targeted by phishing attacks that aim to access student bank account and other information. The goal of the malicious attacks had been to obtain refunds from financial aid proceeds to student accounts.

Bibliography

1. Andersen R. S, Vuori J. and Mutlu C. E. (2015) *Visuality* [in:] Claudia Aradau, Jef Huysmans, Andrew Neal, and Nadine Voelkner (eds) *Critical Security Methods: New frameworks for analysis*, Routledge, London 2015, pp. 85–117.
2. Balzacq T., *The Three Faces of Securitization: Political Agency, Audience and Context*, "European Journal of International Relations" 111 (2/2005), pp. 171–201.
3. Balzacq T. and Dunn Cavelty M., *A theory of actor-network for cybersecurity*, "European Journal of International Security" 1(2) 2016, pp. 176–198.
4. Bleiker R., *Aesthetics and World Politics*, Palgrave Macmillan, London 2009.
5. Buzan B., Wæver O. & de Wilde J., *Security: A New Framework for Analysis*, Lynne Rienner, Boulder 1998.
6. Carlin J., *A Farewell to Arms*, "Wired Magazin", 5 January 1997, https://www.wired.com/1997/05/netizen-2/
7. Carver T., *Cinematic Ontologies and Viewer Epistemologies: Knowing International Politics as Moving Images*, "Global Society" 24 (3/2010), pp. 421–431.
8. Cresswell T. Dixon D., *Introduction: Engaging Film* [in:] T. Cresswell and D. Dixon (eds), *Engaging Film: Geographies of Mobility and Identity*, Rowman and Littlefield, London 2002, pp. 1–10.
9. Dunn Cavelty M., *Cybersecurity Research Meets Science and Technology Studies*, "Politics and Governance" 6 (2/2018), pp. 22–30.
10. Gross M. J., *Stuxnet Worm: A Declaration of CyberWar*, "Vanity Fair" 4 (2011).
11. Hansen L., *The politics of securitization and the Muhammad cartoon crisis: A post-structuralist perspective*, "Security Dialogue" 42 (4–5/2011), pp. 357–369.
12. Hansen L., *How images make world politics: International icons and the case of Abu Ghraib*, "Review of International Studies" 41 (2015), pp. 263–288.
13. Hansen L. and Nissenbaum H., *Digital Disaster, Cyber Security, and the Copenhagen School*, "International Studies Quarterly" 53 (4/2009), pp. 1155–75.

14. Huysmans J., *The Politics of Insecurity: Fear, Migration and Asylum in the EU*, Routledge, London 2006.
15. Massumi B., *From Parables for the Virtual: Movement, Affect, Sensation*, Duke University Press, Durham 2002.
16. Möller F., *Photographic Interventions in Post-9/11 Security Policy*, "Security Dialogue" 38 (2/2007), pp. 179–196.
17. Neal A., *Securitization and Risk at the EU Border: The Origins of FRONTEX*, "Journal of Common Market Studies" 47 (2/2009), pp. 333–356.
18. Neumann I. and Nexon D. (eds), *Harry Potter and International Relations*, Rowman & Littlefield, 2006.
19. Neumann Iver B., *"Grab a phaser, Ambassador:" diplomacy in Star Trek*, "Millennium: Journal of International Studies" 30 (3/2001), pp. 603–624.
20. Parikka J., *Ethologies of Software Art: What Can a Digital Body of Code Do?* [in:] Stephen Zepke (ed.), *Deleuze and Contemporary Art*, Edinburgh University Press, Edinburgh 2010.
21. President's Commission on Critical Infrastructure Protection (1997). *Critical Foundations: Protecting America's Infrastructures*. Washington: US Government Printing Office.
22. Rose G., *Visual Methodologies: An Introduction to Researching with Visual Materials*, 4th Edition (Sage), 2016.
23. Salter M., *Securitization and desecuritization: a dramaturgical analysis of the Canadian Air Transport Security Authority*, "Journal of International Relations and Development" 11 (2008), pp. 321–349.
24. Skibell R., *The Myth of the Computer Hacker*, "Information, Communication & Society" 5 (3/2002), pp. 336–356.
25. Stritzel H., *Towards a Theory of Securitization: Copenhagen and Beyond*, "European Journal of International Relations" 13 (3/2007), pp. 357–383.
26. Weldes J., *Going Cultural: Star Trek, State Action, and Popular Culture*, "Millennium: Journal of International Studies" 28 (1/1999), pp. 117–134.

Appendix 1: Movies

Name	Year	Time	Genre	Plot summary (from IMDB)	Country
1. Tron	1982	1h 36min	Action, Sci-Fi, Adventure	A computer hacker is abducted into the digital world and forced to participate in gladiatorial games where his only chance of escape is with the help of a heroic security program	USA
2. War Games	1983	1h 54 min	Sci-Fi, Thriller	A young man finds a back door into a military central computer in which reality is confused with game-playing, possibly starting World War III	USA
3. Ghost in the Shell 攻殻機動隊	1995	1h 23 min	Animation, Action, Mystery	A cyborg policewoman and her partner hunt a mysterious and powerful hacker called the Puppet Master	Japan
4. Johnny Mnemonic	1995	1h36min	Action, Crime, Sci-Fi	A data courier, literally carrying a data package inside his head, must deliver it before he dies from the burden or is killed by the Yakuza	USA
5. Golden Eye	1995	2h 10 min	Action, Thriller Adventure	James Bond teams up with the lone survivor of a destroyed Russian research center to stop the hijacking of a nuclear space weapon by a fellow agent formerly believed to be dead	UK/USA
6. The Net	1995	1h 54 min	Action, Crime, Drama	A computer programmer stumbles upon a conspiracy, putting her life and the lives of those around her in great danger	USA
7. The Matrix	1999	2h 16 min	Action, Sci-Fi	A computer hacker learns from mysterious rebels about the true nature of his reality and his role in the war against its controllers	USA
8. The Matrix Reloaded	2003	2h 18 min	Action, Sci-Fi	Neo and the rebel leaders estimate that they have 72 hours until 250,000 probes discover Zion and destroy it and its inhabitants. During this, Neo must decide how he can save Trinity from a dark fate in his dreams	USA/Australia
9. The Matrix Revolutions	2003	2h 9 min	Action, Sci-Fi	The human city of Zion defends itself against the massive invasion of the machines as Neo fights to end the war at another front while also opposing the rogue Agent Smith	Australia/USA
10. Live Free or Die Hard	2007	2h 8 min	Action, Thriller, Adventure	John McClane and a young hacker join forces to take down master cyberterrorist Thomas Gabriel in Washington D.C	USA/UK
11. Skyfall	2012	2h 23min	Action, Thriller, Adventure	Bond's loyalty to M is tested when her past comes back to haunt her. Whilst MI6 comes under attack, 007 must track down and destroy the threat, no matter how personal the cost	UK/USA
12. Blackhat	2015	2h 13min	Action, Crime, Drama	A furloughed convict and his American and Chinese partners hunt a high-level cybercrime network from Chicago to Los Angeles to Hong Kong to Jakarta	USA

Appendix 1: TV Series

Name	Year	Number of episodes	Genre	Plot summary (from IMDB)	Country
1. Bloody Monday, Season 1 ブラッディ・マンデイ	2008	11	Action, Suspense	A brilliant high school hacker, Fujimaru Takagi (Haruma Miura), gets drafted by the Japanese equivalent of the FBI(Third-I), to help them stop a group of terrorists intending to attack Tokyo with a biological weapon. When his friends and family members come under attack, Fujimaru realizes the seriousness of the situation he has been asked to participate in. A race against time begins as he helps the Third-I track down those responsible for the impending attack while the true purpose of the terrorist's plan comes to light. Based on the manga, Bloody Monday, by Ryo Ryumon. There is also a sequel involving an aircraft carrying a nuclear weapon heading to Japan.(2010)	Japan
2. Healer 힐러	2014–2015	20	Action, Thriller	A group of friends fight for democracy in South Korea during the Fifth Republic by running an underground radio station to broadcast what is really happening. Decades later an illegal courier, a tabloid website reporter and a broadcast journalist are brought together to solve the mystery of these friends.	South Korea
3. Mr. Robot, Season 1	2015–ongoing	10	Crime, Drama, Thriller	Follows a young computer programmer who suffers from social anxiety disorder and forms connections through hacking. He's recruited by a mysterious anarchist, who calls himself Mr. Robot	USA
4. Pied Piper 피리부는 사나이	2016	16	Action, Thriller	Pied Piper focuses on a police negotiation task force that specializes in tense, worst-case scenarios that require highly trained communication	South Korea
5. Crisis: Special Security Squad CRISIS 公安機動捜査隊特捜班	2017	10	Action, Thriller	A top police official recruits members to s special security team to supposedly investigate crime but really to clean up messes that the police cannot handle or that are deemed to be to dangerous to be conducted publicly	Japan
6. Lookout/ The Guardian 파수꾼	2017	32	Action, Thriller, Drama	A group of people who have lost family members to crimes that the police can't or won't solve gets recruited to work together to solve the mysteries and get revenge by a prosecutor with unclear intentions and a revenge plot of his own	South Korea
7. Final Cut ファイナル・カット	2018	9	Thriller	The protagonist's mother had been accused of a crime that she didn't commit. There was evidence that she didn't commit the crime, but having her the culprit made a better news story. His mother eventually committed suicide because of the media pressure. Fifteen years later, the protagonist begins to execute a revenge plot that has been years in the making when he helps another family that finds itself in a similar situation	Japan