WHAT IS CYBERSECURITY?
In search of an encompassing definition for the post-Snowden era

Morten Bay

UCLA Information Studies
Ph.D. Candidate in Information Studies at UCLA
mortenbay@ucla.edu

Résumé

Le mot ’cybersécurité’ est largement utilisé pour la protection contre les logiciels malveillants et les attaques de pirates. Il est souvent utilisé en situation, dans le sens où les appareils connectés d'un individu peuvent être attaqués, une société peut être piratée ou géréé par le gouvernement, l'infrastructure essentielle peut être l'objet d'attaques. Mais il semble que le terme rende difficile l'exploration d'aspects théoriques de la cybersécurité. Peu de tentatives ont été faites pour comprendre la cybersécurité à partir d'un niveau d'abstraction plus élevé. Dans cet article, il est indiqué que le terme est en effet approprié, car la cybersécurité est un phénomène à multiples facettes qui peut néanmoins être analysé théoriquement à tous les niveaux. La signification du terme est explorée plus profondément et une tentative est proposée pour élargir et approfondir sa portée en tant que concept. La cybersécurité est explorée à partir d'un angle d'études de sécurité critique, ainsi qu'un angle de théorie critique. Une distinction entre les concepts connexes tels que la sécurité de l'information et la sécurité informatique est mise en avant, et une taxonomie de la cybersécurité est suggérée. Il est conclu que la cybersécurité doit nécessairement être analysée de manière critique afin de comprendre pleinement les conséquences et les répercussions qu'elle a en tant que phénomène. Cette analyse va inévitablement conduire à un résultat à multiples facettes, mais sera significative.

Abstract

The word ‘cybersecurity’ is widely used as a term for protection against malware and hacker attacks. It is often used situationally, in the sense that an individual’s connected devices can be under attack, a corporation can be hacked or government-run, essential infrastructure can be at risk of attack. But it seems that the broadness of the term may have made an exploration of the theoretical aspects of cybersecurity difficult. Not many attempts have been made to understand cybersecurity from a higher level of abstraction. In this paper, it is stated that the broadness of the term is indeed appropriate, as

cybersecurity is a multi-faceted phenomenon which nonetheless can be analyzed theoretically across all levels. The meaning of the term is explored further and an attempt to widen and deepen its reach as a concept is made. Cybersecurity is explored from a critical security studies angle as well as a critical theory angle. A distinction of the term from related concepts such as information security and computer security is put forward, and a taxonomy of cybersecurity is suggested. It is concluded that cybersecurity must necessarily be analyzed critically in order to fully understand the impacts and implications it has as a phenomenon, but that this analysis will inevitably lead to a multi-faceted, yet meaningful result.

Cybersecurity is a shared responsibility. The Federal government has the responsibility to protect and defend the country and we do this by taking a whole-of-government approach to countering cyber threats. This means leveraging homeland security, intelligence, law enforcement, and military authorities and capabilities, which respectively provide for domestic preparedness, criminal deterrence and investigation, and our national defense. Yet much of our nation's critical infrastructure and a diverse array of other potential targets are not owned by the Federal government. The Federal government cannot, nor would Americans want it to, provide cybersecurity for every private network. (The White House, 2015)

INTRODUCTION

The quote above is from a press release issued by the White House on February 13, 2015. The occasion was a cybersecurity summit, called by President Obama, which saw participation by leaders from some of America's largest technology-producing and technology-reliant firms. It does not divulge any further information about its last sentence, and why Americans would not want the Federal government to provide cybersecurity for every private network. All-encompassing federal cybersecurity provisions may not be practical, but what is it exactly that makes it so self-explanatory that Americans are against it? In the post-Snowden age, privacy issues come to mind, but also tax payer money being spent on what would essentially be a nationalization of an enterprise that has already been undertaken by private actors in a market worth billions. The White House is most likely correct in assuming that such a policy would be overwhelmingly unpopular. But if that premise is accepted, another, and more complex question is raised: If government, federal or local, cannot provide the citizens it covers with complete protection from cyberattacks, *how much* can and should it provide?

The question is complicated by several factors. When it comes to protection from crime, terrorism or hostile attacks from foreign nations, we rely on the government on protection through law enforcement and the military, two areas that even have their own departments and cabinet secretaries. Even when we employ private protection measures from mall security officers to personal bodyguards, eventually government agencies will take over when incidents happen – from the local police officer that is called in to handle a shoplifter to the arrest of somebody whose attack on a VIP has been

stopped by a bodyguard. But that does not seem to apply as soon as the prefix 'cyber-' is applied. As soon as those five letters are applied to incidents, private actors are in large part the enforcers of protection. It is easy to understand in the case of an attempt to hack an individual's computing equipment – it is analogous to buying home protection through a security firm. But the analogy between 'cyberspace' and 'real-space' does not hold as soon as we turn our gaze to infrastructure. Government entities own and protect infrastructure such as roads, bridges and in some locations, even the power grid in the physical world. But, as the White House press release indicates, there seems to be a perception that digital infrastructures are different, because, A. they are not physical, and B. they are not state-owned or government-controlled and therefore protection of them is first and foremost a responsibility held by the private sector and the government second. In the following, I shall challenge the validity of both those claims.

As the White House press release states, much of critical infrastructure that is targetable through cyberattacks (i.e., digital information infrastructure) is owned by the private sector. A police patrol car can use public streets to move around but the police needs a warrant to search private premises and can only enter them otherwise if there is suspicion of a crime being committed on the premises. But in cyberspace, as the White House admits, all the premises are private, so it is hard for the 'patrol car' to even get to a crime scene. This has led to the government adopting a strategy of what is called "criminal deterrence" in the White House quote above. An interpretation of this term, in the context of the quote, is that the government can react to a crime or an act of war after it is committed, and it can engage in deterrence. It cannot stand in the way of those committing the acts, like it does through national defense. That would require a walled-garden Internet strategy such as the one adopted by China, which is unconstitutional in the U.S., precisely because the infrastructure in question is private. Government attempts to 'patrol' the infrastructure are massively unpopular, as the Snowden case has revealed (Ganguly, 2015). Which raises another question: How can the government act as provider of *any* type of security, if it is not allowed some amount of surveillance power, i.e., the ability to monitor what is happening in the digital infrastructure?

What all this rather simplistic reasoning adds up to is the fact that the analogy between 'real-space' and 'cyberspace' (see definitions below) does not hold by default. There seems to be a need to treat the 'cyber' realm differently and rethink the way justice is enforced and international relations are maintained. Every U.S. citizen has a constitutional right to protection against both crimes and acts of war from the government. The constitution's preamble states that the government by the people shall "establish Justice, insure domestic Tranquility, provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity" (Archives.gov, 2015), so the government cannot be left completely out of the picture, even when it comes to the 'common defence' and 'securing the Blessings of Liberty', a task which it would seem falls to private actors in the digital space.

In other words, it appears that there is a need to examine the term 'cybersecurity' and move towards a more specific understanding of the concept, which encompasses both the cybersecurity provided by private actors, as well as the cybersecurity provided by government agencies, in order to protect the lives, property as well as privacy for individuals in the network age.

WHAT IS CYBERSECURITY?

The word 'security' is defined in the online version of the Oxford English Dictionary (Oxford University Press, 2015) as "The state of being free from danger or threat". However, that simple definition belies the complexity of the actual use of the word, and particularly when it comes to *cyber*-security. The latter term is used continuously by politicians, computer specialists, IT managers, tech entrepreneurs, health industry professionals and national security operators, a spectrum so wide it would seem almost impossible that so many people would agree on a definition. As it turns out, there are differing views on what cybersecurity is. The term is used to cover the measures government institutions take to protect the public and the institutions themselves from threats in the 'cyber'-domain, also known as 'cyberspace'. Yet it is also used on a level that is somewhat closer to the individual, when it refers to protection against viruses and other malware on a computer, whether this is personally owned or used in the work situation.

The term itself also does not give any clues as to which threats, cybersecurity secures *against.* Unlike a term such as 'national security,' 'job security' or 'environmental security' which clearly state that the things to be secured are the nation, employment and the environment, cybersecurity is less clear. Is it 'cyber' that needs protection, or is the security put in place through means of 'cyber'? Since its emergence in the years following the end of the cold war (see below), attempts at interpreting and defining cybersecurity have been made by many scholars. In the following I will provide an overview of the movement towards a more specific definition of cybersecurity, beginning with the breakdown of this composite into its two components, followed by a discussion of the term as a whole.

DECOMPOSING CYBERSECURITY

Most state-provided/ public definitions of cybersecurity can be classified as realist/positivist as I will explain below. This so-called traditional view on security writ large is mostly oriented towards threats at a systemic/collective level, rather than an individual level. This means that usage of the term by public officials or public communication outlets usually does not address the individual's need for cybersecurity on his or her computer (or other device), but rather it addresses the cybersecurity needs of the nation, larger population groups, infrastructure critical to the population or to businesses and the general economy. This way of addressing the issue resembles the rhetoric surrounding national security in the offline world, and it is not surprising that there is a parallel between this (particularly the U.S. government's) way of addressing cybersecurity and traditional/realist/ positivist notions of security as such.

An example could be US-CERT (United States Computer Emergency Response Team), the cybersecurity division of the Department of Homeland Security (DHS), which offers both a broad and a more specific definition online:

> *"The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."*

> *"Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. (DHS, 2015)*

From a scholarly standpoint, Craigen, Diakun-Thibault, and Purse (2014) define the term in a way which attempts to cover as much ground as possible, and yet still have a legalistic resonance: "Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights" (p.1).

WHAT IS CYBERSPACE?

However, this definition does not make much sense without a clear definition of "cyberspace," and most other definitions of cybersecurity discussed here are also contingent on an understanding of that term. The term is most often attributed to Science fiction writer William Gibson's novel *Neuromancer*, in which 'cyberspace' is presented as a virtual, three-dimensional space consisting entirely of information (Gibson, 1984), but Gibson actually introduced it in the short story *Burning Chrome* two years earlier (Gibson, 1982). The concept is also presented by Vinge (1981) and Ford (1980). Since then, it has been appropriated by the broader public, and the Oxford English Dictionary online now defines it as "The notional environment in which communication over computer networks occurs." (Oxford University Press, 2015). This is not a very useful definition, particularly since the meaning of "computer networks" is not explored further, and since more and more things which one would be hard pressed to call "computers" are now communicating via the same networks as computers (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Tan & Wang, 2010).

Scholars have attempted to approximate a more precise definition such as Lorents and Ottis (2010): "Cyberspace is a time-dependent set of interconnected information systems and the humans that interact with these systems" (p.1). Here, the users are considered part of cyberspace in an almost Latourian actor-network relation (Latour, 2005), or even the symbiotic state described by Licklider (1960) in one of the earliest papers on humans and networked computing. Others, such as Strate (1999), define cyberspace as an imaginary, socially constructed concept, supported by infrastructures such as the Internet. However, Craigen, Diakun-Thibault, & Purse finds that the term has evolved:

> *What we now know as cyberspace was intended and designed as an information environment …and there is an expanded appreciation of cyberspace today. For example, Public Safety Canada (2012) defines cyberspace as "the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where… people are linked together to exchange ideas, services and friendship." Cyberspace is not static; it is a dynamic, evolving, multilevel ecosystem of physical infrastructure, software, regulations, ideas, innovations, and interactions influenced by an expanding population of contributors…who represent the range of human intentions. (p.2)*

WHO IS CYBERSECURE?

So the aforementioned dichotomy between systemic/collective cybersecurity add individual cybersecurity has a parallel in the definitions of 'cyberspace'. Public Safety Canada (2012) as well as Lorents and Ottis (2010) regard humans/individuals as meaningful and essential elements in the structure of cyberspace, whereas DHS (2015) and Craigen, Diakun-Thibault, and Purse (2014) define it more in terms of systemic structure. Diplomatically, the international standards organization attempts to straddle this divide by defining cybersecurity simply as: "Preservation of confidentiality, integrity and availability of information in the Cyberspace" (ISO, 2015), which can be understood both in collective as well as individual contexts. Note that this definition is focused on information, and the cybersecurity definition is in fact simply an adjusted version of the ISO's definition of 'information security' (I shall return to the difference between the two later). The DHS does not include people/users in their definition of neither cybersecurity nor cyberspace. But interestingly, users are mentioned in the cybersecurity interpretation of 'situational awareness' in the official DHS glossary. "In cybersecurity, comprehending the current status and security posture with respect to availability, confidentiality, and integrity of networks, systems, users, and data, as well as projecting future states of these." (DHS, 2015, section "C")

In other words, it is fair to conclude that these examples from the very different domains of business standards, national security and critical, scholarly work, all have one thing in common: they see cybersecurity as either being the security of systems or individuals as part of (or being connected to) the systems. This dichotomy has recently become the subject of debate in the more general field of security studies, and is quite essential to the aim of this document. Application of critical theory to the security studies field has shed light on the importance/relevance of the dichotomy between systems and people when it comes to security policy. But to further explore that discussion, we must first dive deeper into the meaning of cybersecurity to completely understand the tensions and conflicting views that live within the concept. I shall start by breaking down the term into its two components.

WHAT IS 'CYBER'?

Cybernetics

The term 'cyber' as a prefix has a long and somewhat colorful history. There seems to be broad consensus that the origin of the usage of 'cyber' is Norbert Wiener's (1948) coining of the term 'cybernetics' (Bowker, 1993; Ottis & Lorents, 2010; Geoghegan, 2008; Peters & Geoghegan, 2014), but the consensus does not extend to the actual definition of the term. In fact, as Umpleby (2000) shows, there has been a number of different definitions put forth over the course of the last 70 years. These range from the ethereal to the more concrete definitions, the latter of which tend to have a connection or residence with Wiener's original use of the word. In etymological terms, Wiener wrote:

> *I first looked for a Greek word signifying 'messenger' but the only one I knew was angelos. This has in English the specific meaning 'angel', a messenger of God. The word was thus pre-empted and would not give me the right context. Then I looked for an appropriate word from the field of control. The only word I could think of was the Greek word for steersman, kybernetes (Wiener 1956, p. 322)*

Wiener was concerned with the relationship between animals and (mostly mechanical) systems, and the feedback of information between them. He saw this interaction as having direction as the feedback causes reiterations in the process. This is why he was drawn towards using the Greek word for 'pilot' or 'steersman.' At the Macy Conferences between 1946 and 1953, the concept was developed further by Wiener in collaboration with influential thinkers such as Margaret Mead, Gregory Bateson, Claude Shannon, John von Neumann, Warren Weaver, Warren McCulloch, Walter Pitts and others, and a more human/machine- focused notion of cybernetics emerged, in which "machines are active agents in their world, whose behavior provides insight into the structures, constraints, and laws of human society" (Peters & Geoghegan, 2014, pp. 111). Research in cybernetics was also performed in the Soviet Union in the 50s and 60s, making it one of many research areas of concern in a cold war context (Holloway, 1974; Peters & Geoghegan, 2014).

Birth of the cyborg

In 1960, the discourse on cybernetics led Clynes and Kline (1960) to propose the word 'cyborg' (a subtraction of 'cybernetic organism') as a description of a being that "deliberately incorporates exogenous components extending the self-regulatory control function of the organism in order to adapt it to new environments" (p. 27). This spawned a decades-long fascination with cyborgs within both popular culture and critical, academic discourse. Hayles (1999) traces use of the concept (without the term) in popular culture as far back as 1952 and the Bernard Wolfe novel *Limbo.* In film and TV, cyborgs (named 'cybermen') appear as early as 1966 in the television series *Dr. Who,* and in 1973, the TV series *The Six Million Dollar Man* was based on Martin Caidin's 1972 novel *Cyborg.* Later came more prominent pop culture cyborgs such as Darth Vader in *Star Wars* (1977), the T-800 model 101 in *The Terminator* (1984) and Alex Murphy in *RoboCop* (1987).

In academia, the cyborg concept inspired Donna Haraway (1991) to use the conjoined nature of cyborgs as a metaphor for how divergent discourses in feminism can be symbiotic, but also as a symbol of masculine dominance in informatics and as the end result of capitalism's treatment of humans. So-called German media theory and the media archaeology of Friedrich Kittler is also a result of the cybernetics discourse, at least according to Peters & Geoghegan (2014), although this is debatable, considering media archaeology's analytical focus on the materiality of information and the media that conveys it. Peters & Geoghegan also find cybernetic modeling in the French postmodernist/poststructuralist movement in the 80s and 90s, both in the semiotic analyses of Barthes and Beaudrillard as well as in the general technocratic critique of the movement.

As a prefix

But what of 'cyber' as a prefix applied to existing words? The earliest use found in The Oxford English Dictionary (2015) is from a 1966 issue of *New Scientist*, where the term 'cybernoracy' is mentioned. It then goes on to cite Douglas Adams' classic *Life, the Universe and Everything*, the second sequel to *The Hitchhiker's Guide to the Galaxy*, for use of the word 'cybercubicle' in 1982. The OED's general definition of 'cyber' as a prefix is "Originally: forming words relating to (the culture of) computers, information technology, and virtual reality, or denoting futuristic concepts. Later also: spec. forming terms relating to the Internet." The latter, according to the OED, is probably inspired by the word 'cyberspace,' which (as mentioned earlier) William Gibson introduced in his 1982 book *Burning Chrome* (Gibson, 1982), after Vernor Vinge had introduced the same concept a year earlier under another name, 'Other Plane' (Vinge, 1981).

Borgman (2007) shows how 'cyber' is often used interchangeably with the 'e-'-prefix, and how the latter is used more often in Europe, whereas the US prefers 'cyber' (something that Borgman asserts is rooted in the government's upholding of the term 'cyber', which fell out of fashion and then re-emerged in academia). Borgman also attributes the emergence of the 'cyberpunk' genre to William Gibson's work, a genre which has since been said to include a slew of films and books. Timothy Leary (1988) personalized 'Cyberpunks', defining them as an individuals who "use all available data-input to think for themselves" (p. 252). He later goes on to state that Christopher Columbus was a cyberpunk in the sense that he uses both data and data-producing technologies to navigate his way through space as well as life. 'Cyberpunk' has also been mentioned as a name for a musical genre (which is actually the synth-driven New Wave/New Romantics movements of the early 1980s), as a prominent writer in the cyberpunk *literary* genre, Pat Cadigan, recalls:

> *One morning in 1979, I was getting ready for work and Gary Numan's "Cars" came on the radio. Afterwards, the DJ said, "There's some cyberpunk for you." He was making a joke; in 1979, the punk movement was in full flower but the chaotic noise of punk music was starting to evolve into electronic noise. (Newitz, 2013)*

Leary's and Cadigan's definitions are good examples of how widely the 'cyber' prefix is used and how far it has traveled from Wiener's original use of the word 'cybernetics'.

The prefix is "now widespread in the description of electronic and digital phenomena" (Peters & Geoghegan, 2014, p.1) and as Ottis and Lorents (2010) notes: "In recent years the term "cyber" has been used to describe almost anything that has to do with networks and computers" (p.1). Nguyen (2013) believes that "Scholars writing in this area over the last decade have abandoned the use of "computer network attacks" in favor of the more fashionable prefix "cyber-" (p. 1088). Cavelty (2012) employs an even wider usage and states that 'cyber' "has a general meaning of 'through the use of a computer'", but also finds that 'cyber' is "used synonymously with "related to cyberspace" (p. 4). Craigen et al. (2014) cite Cavelty, but build on the latter part of her definition, calling 'cyber' "a prefix connoting cyberspace and refers to electronic communication networks and virtual reality" (p.14).

From this discussion, and particularly the last few remarks about the prefix 'cyber', it seems that the use of the prefix is broadly used to relate the word following the prefix to either cyberspace, virtual reality or computers more broadly. As virtual reality is sometimes dependent on cyberspace, but always contingent on the presence of computing equipment, it is included in at least one of the two other connotations. That leaves us with 'cyber' denoting either a connection with cyberspace or computers more broadly. Going forward, however, I shall be using the prefix as it relates to cyberspace, i.e., not just computers more broadly, but connected computers. This is because, as I shall argue, there is an important difference between cybersecurity and computer security. Computers can be insecure without being connected, and using 'cybersecurity' in the context of insecure, but disconnected computers invalidates the relationship between 'cybersecurity' and 'cyberspace'. Since this text is concerned with cybersecurity, I shall therefore use the term 'cyber' only in relation to computers that are in some way part of cyberspace.

WHAT IS 'SECURITY'?

While the term ' cyber' is relatively simple to deconstruct, the term 'security' appears to be more complex. As mentioned above, the first definition of the word 'security' in the Oxford English Dictionary (2015) states that it is a state of protection from threats. But there is in fact a whole field dedicated to the study of security. Security studies exists as a subfield of international relations within political science, and in recent decades, the field has been expanded with theories of a more critically theoretical nature, linking it to more traditional areas of critical studies (Wæver, 2004).

Peoples and Vaughan-Williams (2015) provide an overview of the current theories in security studies, identifying eight dominant schools of thought within the field. The Aberystwyth, Paris and Copenhagen schools combine with constructivist, postcolonialist and feminist angles on security studies to form a category the authors refer to as critical security studies. These schools are somewhat Euro-centric, and are in opposition to what the authors consider an American approach, based on realism and positivism, and labeled traditional. (Peoples & Vaughan-Williams, 2015, p. 21). As will become apparent from the description of each of these schools of thought that I provide below, the traditional school is rooted in post-World War II concepts of security, understood as *national* security as it emerged during the cold war era.

Security studies schools of thought

As pointed out by Buzan and Hansen (2009), it is only in the last two decades that the field of security studies has been expanded with critically theoretical approaches. Before this relatively recent development, security studies were primarily nation-centric, which also meant that it dealt with national security, which in turn meant that the discussions of military power and strategy dominated the field. This is now known as *traditional* security studies in contrast to the contemporary *critical* security studies.

The authors note that the modern conception of international relations studies has its roots in the development of the modern state. They describe the evolution from the chaos of medieval, regional rule, over the formation of the monarchic state to the popular nation-state of today, of which many (at least in the West) can point to the Enlightenment period as the time of emergence. They see the 1648 Treaty of Westphalia as a line in the sand, after which European nations no longer would interfere in each others' religious choices. From then began the long journey towards what the authors call the "sovereign territorial state" (Buzan & Hansen, 2009, p. 24), the basis for international relations and hence also for security studies.

Traditional security studies

The primary schools of thought in traditional security studies are the *strategic studies* and the *realism* schools, as described below.

Strategic studies

As the name implies, this is the Study of strategies for obtaining security based on the security dilemma. The latter term was coined by John Herz (1951) and describes the following situation: When one nation competes for security (that is, seeks to achieve security from existential threats) , it inadvertently raises the insecurity of other nations in the international political system of which it is a part, with more tensions as a consequence. With no unit of sovereignty above the sovereign nations in the international political system, the latter is in fact a system of anarchy, with only alliances and treaties to keep chaos at bay. During the cold war, this anarchic state of existence slowly evolved into a situation of bipolarity, with two superpowers competing to obtain a sovereignty-by-alliance by creating alliances with sovereign states. This bipolarity dominates Strategic Studies, particularly and watch some referred to as (international) security studies' "golden age" (Buzan & Hansen, 2009, p. 67). It is in this era that now well-known strategic methodologies such as 'The Prisoner's Dilemma' and game theory (which are mostly contingent on bipolarity) emerge from strategic studies (p.69). This is an expression of a predominately realist/positivist approach to security, with empirical/mathematical modeling methodologies as the main drivers. Strategic studies saw as its main sector of concern the use of military force, and was predominantly state-centric.

Realism

Alongside strategic studies in the traditional category is the school of realism, divided up into classical and neorealism. The former is a sort of revival of pre-Enlightenment strategies in international relations inspired by writings from sources such as Machiavelli and Hobbes. Classical realists assume a Hobbesian 'state of nature' and the derived human nature to be the driver of decisions that lead to

war (Buzan & Hansen, 2009). After World War II, this brand of realism was rediscovered by scholars such as Hans Morgenthau (1948) and Reinhold Niebuhr (1952). Classical realism was later succeeded by neorealism, with Kenneth Waltz (1979) as its main proponent. Waltz replaces human nature with the pressures and tensions created by the anarchic state of existence described under strategic studies as the main driver for conflict. It is also state-centric approach, but rather than rely on military force as the only tool, realist security studies also consider the political/diplomatic sectors as influential and powerful entities that can be entered into the methodology. Also, rather than relying on mathematical modeling and empirical data, this school has a rationalist angle, viewing nations as rational actors, rather than attempt to model their behavior (Buzan & Hansen, 2009; Waltz, 1979).

Peace research

Opposed to these two schools, the peace research school also emerged as a part of the traditional security studies domain during the cold war. Like strategic studies, this school has a primarily positivist view, using empirical data and game-theoretic modeling to support its theories. The positivist view was also strengthened by the major participation of Marxist materialists in this school in the 50s, 60s and 70s. Like strategic studies, it is interested in the nuclear arms race, but with the stated mission of control and future disarmament. In contrast to strategic studies, it includes societal and individual concerns alongside state/national interests and is the only school in the traditional category to do so. It seeks to employ all sectors of government in order to achieve peace, and instead of taking a realist stance, it presents the possibility of transformation rather than accepting reality as it is. Where strategic studies and realism were primarily Anglo-American phenomena, peace research was mostly Northern European, with strongholds in Scandinavia and Germany (Buzan & Hansen, 2009; Peoples & Vaughan-Williams, 2015)**.**

Critical security studies

The Aberystwyth school

Also referred to as the 'Welsh' school, this theory was the first to employ a critical approach to security studies. It is also known as CSS – Critical security studies (note the capital C, which distinguishes the school's name from the general category.) Formed from a discourse between scholars at Aberystwyth University in Wales, CSS broadens and deepens the concept of security to go beyond the nation-state (Peoples & Vaughan-Williams, 2015, p. 60). CSS focuses instead on the security of people, and on threats that are "real ones against real people and not the allegedly real ones voiced by the state" (Wæver, 2004, p. 7). CSS scholars use the term 'emancipation' for this shift in focus.

The Copenhagen school

Ole Wæver, Lene Hansen and Barry Buzan are some of the scholars that are most often tied to the Copenhagen school. It is best known for its theory of 'securitization', as presented by Wæver (1995), in combination with the idea of studying security as being of different kinds, depending on the field, as suggested by Buzan (1991). 'securitization' is a Austinian speech-act according to Wæver, who suggests that by talking about something in connotation with the word 'security', we performatively lift it out of the realm of political discourse or political theory and into a separate security discourse. This matters in the same sense that CSS shifts the focus from nation-states to people. Wæver's view is

that the security discourse is much more restrictive than the political discourse, which is where Buzan's theory of different securities, and how to identify a security issue, comes in.

In its essence, Buzan claims, security is fundamental matter of survival, and as such security is only concerned with existential threats. But these threats can be to the existence of things, peoples, organizations or concepts, not just living beings (Buzan, 1991). Buzan uses a term commonly employed by critical security studies scholars for that which is in need of security: 'Referent object', i.e., in this case, the existentially threatened entity. Securitization is thus the process of assigning existential threats to something and discourse, and the consequences of this speech-act. When one assigns an existential threat to, e.g., a state as an entity, it becomes a matter of national security, and securitization becomes foundation for a national defense apparatus with the economic and social implications that entails (Peoples & Vaughan-Williams, 2015).

But it is important to note that the Copenhagen school's securitization concept opens up security discussion to other contexts other than strategic security, such as environmental security or economic security, both of which address grave threats to the well-being of humans and stability of their society – just like national security (Buzan & Hansen, 2009). In summary, the securitization theory of the Copenhagen school is about the performative discourse on security and how it impacts actual, real security issues. It is unsurprising that Foucault is often mentioned as an influence on the Copenhagen school (see Wæver, 1990, 2004), whereas the Frankfurt school brand of critical theory has more of an impact on Aberystwyth (Wæver, 2004).

The Paris school

This French version of security studies is often referred to as a poststructuralist, and sometimes a sociological approach to the field. As the name implies, the French tradition of critical thought as prevalent here, and influences from postmodernists/ poststructuralists from Derrida to Baudrillard are attributed to the Paris School, but, as we shall see, the sociological approach may have an even deeper footing in this particular school of thought. In the poststructuralist mode, the Paris school is mostly focused on typical poststructuralist tenets such as discourse and deconstruction.

After the end of the cold war, decades of a classic, singular-enemy view on security had to be dismissed. According to Peoples and Vaughan-Williams (2015), poststructuralists jumped at the chance to deconstruct this classic paradigm, and analyze the discourse on security as such. The events of 9/11 provided even more reasons for deconstructive analysis, as the nation-State was replaced by the concept of terror as a main threat to national security, and enemies were personified as individual members of transnational terror organizations. This particularly led to a poststructuralist deconstruction of the so-called 'inside/outside' division of security enforcement. This concept defines defense institutions such as the military as dealing with threats from the outside, while securities from different types of threats inside society is upheld by civil institutions such as the police, the courts etc. With the emergence of terror as an 'enemy-concept', this division no longer applies, or at least its dividing line is blurred. If an individual detonates a suicide bomb on the street in a major, western city, it is technically an 'inside' security issue. But if that individual is connected to, and motivated by, a terror organization, the doctrine of the Bush era in the early part of the century dictates that it is also an outside security issue. The classic security paradigm off the cold war has deconstructed itself completely.

This view is put forth by another theorist, who is actually more grounded in a separate French tradition, and who has become the main thinker of the Paris school of security studies. Didier Bigo's influences are Bourdieu and Foucault, rather than prominent poststructuralists. With his focus on practices, Bigo's work has been described as International political sociology (IPS) (Peoples & Vaughan-Williams, 2015). Bigo uses Bourdieu's concepts of field and habitus as well as Foucault's idea of the individual as an actor that engages in a constant flurry of power transactions to create a theory of security which is actually focused on the opposite: insecurity. In the same way the Copenhagen school views securitization as a speech-act that enables security measures, Bigo talks about a sort of 'insecuritization': "The actors never know the results of the move they are making, as the result depends on the field effect of many actors engaged in the competitions for defining whose security is important and by the acceptance of different audiences of their definition." (Bigo, 2008, p. 124). Thus, Bigo views the field as being so chaotic (because of the deconstruction of the habitus off the post-9/11 world) that it is hard for anyone to achieve security, either as individuals or as nations. Bigo's partial dissolution of the inside/outside distinction is essential to the discourse on cybersecurity, as we shall see further along in the text.

The constructivist approach

Two leading figures in the constructivist approach to international relations and security studies are Alexander Wendt and Ted Hopf. These two scholars are in slight opposition to each other, in the sense that Wendt's constructivism is seen by Hopf as being too close to traditional security studies to be considered critical. However, they both share a view of security studies which focuses on the analysis of security issues and institutions as social constructs.

To understand this approach, it may be useful to begin with Wendt and his view of the security dilemma, as described previously. According to Wendt, this is in fact a social construct more than unchangeable reality, such as it is presented by Herz. To Wendt, a security dilemma is really a "social structure composed of intersubjective understandings in which states are so distrustful that they make worst-case assumptions about each others' intentions, and as a result define their interests in self-help terms" (Wendt, 1995, p.73). This is an example of how Wendt sees national security and the threats to it as social constructs. In the constructivist approach, nation-states can also be viewed as social constructs, which defines security almost in structuralist terms. Wendt also shows how the means of security enforcement, such as military equipment, only have meaning within a certain epistemological construction: "material capabilities as such explained nothing; their effects presuppose structures of shared knowledge, which vary and which are not reducible to capabilities" (Wendt, 1995, p. 73).

As mentioned, Hopf (1998) does not believe that Wendt goes far enough in his constructivist analysis. He suggests an even more critical approach, which attempts to decompose even further the issues and institutions of security. Hopf, along with Weldes et al, (1999) talks about the social production of danger and insecurity (overlapping slightly with Bigo), and wishes to further unmask the structures of security, as well as be critical of the intellectual foundations of mainstream International Relations theory as well as traditional security studies, and even critical, constructivist security studies itself (Hopf, 1998, Weldes et. Al 1999).

The feminist approach

Even a brief exploration of traditional security studies should make it quite obvious that there is a need for a feminist critique of the field. More than two decades ago, Enloe (1989) showed how the field skews male when it comes to scholars in the traditional security studies category. This may seem like a logical extension of the fact that there is male dominance in security enforcement institutions and particularly in outwardly facing security institutions such as the military. With only 14.6% of those serving in the US military being women (DoD, 2013), it is hard to argue that there is not male dominance, and that the likelihood of a patriarchy being in place isn't high. With the emergence of critical security studies and the feminist approach however, the structures are being challenged. Enloe (2000) shows that it is not only in the military or in military leadership that this inequality exists, but also in international politics in general.

Moreover, the feminist critiques in security studies also theorize that certain parts of the discourse is seen by many as having masculine connotations. Tickner (1992) shows how even the perception of the word 'international' is associated with traits such as strength, power and autonomy, which she asserts is associated with masculinity. She also refers to the "essentialist connection between war and men's natural aggressiveness" (Tickner 1992, p. 72). This critique of gender attribution to elements of security studies, is at the heart of the feminist approach, as is the more realist-feminist critique of the patriarchy in security institutions.

The postcolonialist approach

Like the feminist approach, the postcolonialist approach seems to have an obvious reason to exist. In traditional and realist security studies, the socioeconomic conditions of nations are central to the analysis of security issues. But as it is often the case, there is an alternative view on how to perceive discourses on subjects such as 'the third world' or 'the global south.' Even the critical side of security studies can be viewed as very western-centric. As Ole Wæver (2004) puts it: "Why in Aberystwyth, Paris and Copenhagen – why not in Amman, Philadelphia or Calcutta?" (p. 2). Wæver notes that the emancipatory theory of CSS may seem useful to regions outside Europe and the US, at least when seen from those two vantage points. However, he cautions, "Especially in Latin America, there is a wide-spread consciousness about the ways security rhetoric has been used repressively in the past, and therefore a wariness about opening a door for this by helping to widen the concept of security" (Wæver 2004, p. 24).

Unsurprisingly, postcolonial critiques of security studies also come from outside the first world. Ayoob (1997) cautions against the "fashionably expansionist definitions of the concept of security" (p.139), and calls for a "subaltern Realism" which may be conducive to a more tailored discourse on security, better fitting the concerns and issues facing nations outside the US and Europe. Many other scholars echo this sentiment, but at this point I shall refrain from driving further into this approach to security studies, since I will revisit the matter later in the text in another context.

CYBERSECURITY VS INFORMATION SECURITY

Cybersecurity and information security are two distinct fields of study that nonetheless are often conflated (von Solms & van Niekerk, 2013). In the following I will demonstrate why it is important to make clear distinctions between the two, but also show where they overlap, in order to further move towards a workable definition of cybersecurity.

Formal difference

The International Standards Organization (ISO) (2014) defines *information security* as:

> *Preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information.*
>
> *Note 1 to entry: In addition, other properties such as authenticity (2.8), accountability, non-repudiation (2.54), and reliability (2.62) can also be involved. (p. 4)*

ISO's definition of cybersecurity is quite similar: "Preservation of confidentiality, integrity and availability of information in the Cyberspace" (ISO/IEC, 2012, section 4.2). ISO also has a definition for what it calls "the Cyberspace": "The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form" (ISO/IEC, 2012, p. 5). The difference in the formal definitions from ISO is clear, in that cybersecurity is simply information security in cyberspace, the latter being defined as physical entities connected via the Internet, as well as the Internet itself.

Blanchette (2011) argues that such aphysicality does not exist within the ITC realm, but even if one accepted the physicality/materiality that would still be a substantial difference between these two definitions. The ISO's definition of cybersecurity places emphasis on non- materiality, but it also places emphasis on connectedness, whereas the definition of information security does not. Not all information is stored in repositories which are accessible via digital networks such as the Internet, and so the connectivity of cybersecurity distinguishes it from information security in ISO's formal sense.

Historical difference

Information security is also a substantially older concept than cybersecurity. As Lehtinen (2006) points out, telegraph messages could be encrypted to ensure privacy in the communication from the very invention of the telegraph in the 1840s. Even Julius Caesar applied code to the messages he dispatched out into the Roman Empire via messenger in the 1st century. (Dlamini, Eloff & Eloff, 2009). As noted elsewhere in the text, the prefix 'Cyber-' does not appear until Wiener's use of it (1948), and though sources disagree on the first known use of the word cybersecurity, it seems to have emerged somewhere in between 1989 and 1994 (see Merriam-Webster, n.d.; Newitz, 2013; Zimmer, 2013). Cavelty (2012) traces the discourse – not the term – on cybersecurity back to the 1970s. But in either case, cybersecurity has become a widely used term in recent decades, whereas information security dates back more than a century. Since the concept of information security still exists and has

not been replaced by cybersecurity (for the difference reasons stated above), there is also a disparity between the two concepts historically.

Topical difference

Upon further analysis into the actual meaning of the terms, differences also start to appear. Von Solms & van Niekerk (2013) shows that, although there are many similarities, there are also plenty of examples where a breach of cybersecurity is not the same as a breach of information security:

> *If cybersecurity is synonymous with information security it would be reasonable to assume that cybersecurity incidents could also be described in terms of the characteristics used to define information security. Thus, a cybersecurity incident would, for example, also lead to a breach in the confidentiality, integrity or availability of information. (p.99)*

The authors then go on to present a number of scenarios that

> *…deal with a specific aspect of cybersecurity where the interests of a person, society or nation, including their non-information based assets, need to be protected from risks stemming from interaction with cyberspace. This serves to highlight the difference between information security and cybersecurity (p.100).*

Generally, von Solms & van Niekerk conclude that the main difference in the natures of information security and cybersecurity is that information security is focused on the protection of the actual information itself, where as cybersecurity is concerned with the information infrastructure, and what is reachable through the infrastructure (which is not exclusively information):

> *Information security is the protection of information, which is an asset, from possible harm resulting from various threats and vulnerabilities. Cybersecurity, on the other hand, is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace and any of their assets that can be reached via cyberspace. (p. 101)*

With the number of devices connected to networks and the Internet growing, not least because of the emergence of the so-called 'Internet of Things', it is clear that information is not the only vulnerable assets in need of protection online (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015; Tan & Wang, 2010).

CYBERSECURITY VS COMPUTER SECURITY

Matt Bishop insists on using the terms 'cybersecurity' and 'computer security' interchangeably (Bishop, 2003, 2005; Talbot, Frincke, & Bishop, 2010). However, this is highly problematic when trying to define cybersecurity as an object of study. Just as information in itself is separate from the information infrastructure and the two can be studied separately, so are computers also separate from the information infrastructure, even if they may be connected to it. To put it another way, computers can be insecure without being connected, and be under similar threats without ever touching the Internet. One of the most famous examples of this is the Stuxnet malware which was used to bring a uranium enrichment facility in Iran to a halt. Stuxnet was introduced to the facility's internal network, which is not connected to the Internet, and from here it was able to spread to the computers controlling the enrichment process, shutting them down. This introduction happened by way of an 'airgapped' laptop computer (a computer who which has never been connected to the Internet), which is thought to have been compromised through the insertion of a infected USB stick (Denning, 2012; Richardson, 2011). However, as I have suggested elsewhere, and will continue to establish below, the cybersecurity term should only apply to computing machinery in cyberspace, i.e., the Internet and its connected entities. Since one of the most notorious malware attacks happened without the Internet ever being involved, it is easy to argue that the need for computer security exists separately from cybersecurity. The two overlap in the cases of computers that are connected to the Internet.

Another problem that arises when cybersecurity is conflated with computer security is the definition of the computer itself. Bishop does not provide one such definition, which raises the question of whether any device utilizing a traditional computer architecture, such as the von Neumann architecture, can be called a computer. If this is the case, computer security must encompass devices such as tablets, smartphones, e-readers, smartwatches, but more importantly also many of the aforementioned devices connected to the Internet of Things. These include home automation system devices such as locks, light bulbs and thermostats, and a whole host of entertainment devices. What makes these devices 'smart' are their ability to function like a computer, but also their connectivity. Many of them lose their *raison d'être* if they are not able to receive information from the Internet, which – in the ISO definition - makes them a part of cyberspace. So even though the security of these devices *may* be covered by the term 'computer security', they are *certainly* covered by the cybersecurity term. In Fig. 1 below, the distinctions are illustrated by a Venn diagram.

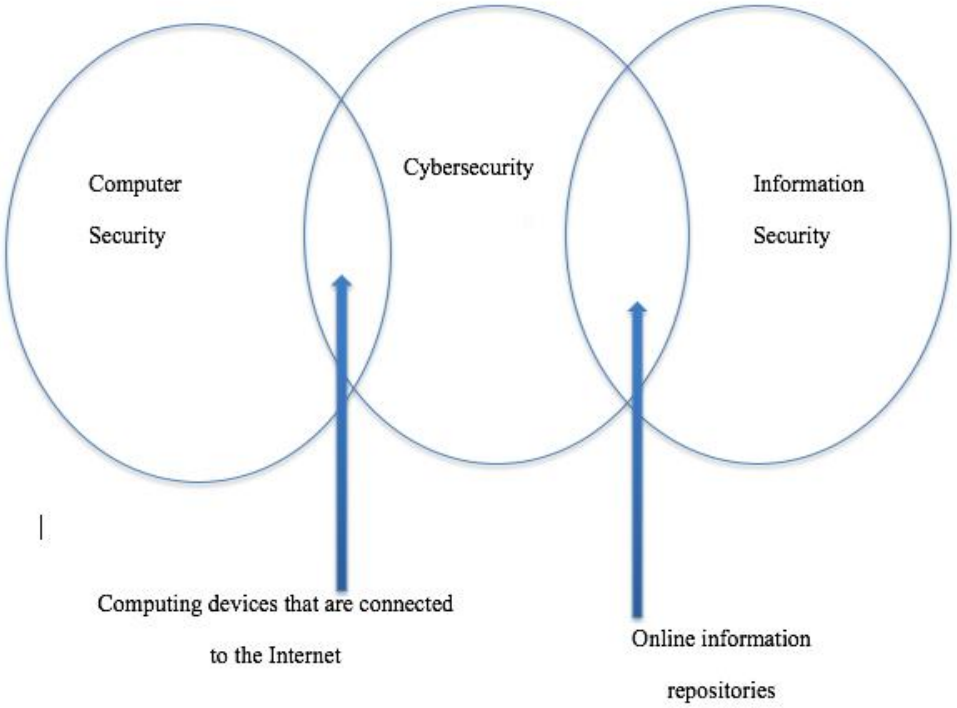

Fig.1 The relationship between computer security, information security and cybersecurity

Threats To Cybersecurity

As I have shown in the section defining the concept, security exists only in lieu of the existence of *threats*. In the following, I will attempt to break down the threat concept in a cybersecurity context, leading to a workable definition of the term 'cyberattack', which I will assert is a more precise and useful term to use in the discourse on threats to cybersecurity.

Threat Taxonomy

A host of cybersecurity-related terms are used in literature and public communication that are (like the term cybersecurity itself) not necessarily well-defined, and particularly the commercial side of the cybersecurity domain seem to allow for the constant creation of new buzzwords for marketing purposes. However, there seems to be some consensus around a few classifications of computer network threats. In the following, I shall introduce those of the threat distinctions which are relevant for this review and suggest a taxonomy to distinguish them from each other.

Terms. *Cybercrime; Cyberterrorism; Cyberwarfare; Cybervandalism / Cyberactivism; Cyberespionage*

All these words are representative of some sort of cyber-*activity* or cyber-*action*. Other words describing the units which would be classified under these terms are "cyber-event", 'cyber-incident',

'cyber-conflict' and 'cyberattack'. For the purposes of this paper, however, and in line with the above attempt at defining the terms used here more precisely, I find 'cyber-event', 'cyber-activity', 'cyber-action' and 'cyber-incident' to be too generic. They may cover the simple transmission of a bit or the actions of piece of protocol software without any indication of it happening in good or bad faith. As with most network activity, these are value-neutral events and therefore hard to classify within the five categories above, as these all pertain to some sort of operation which – for whatever purpose – seeks to inflict damage. 'Cyber-conflict' is also problematic. Can digital identity theft and following financial damage to an individual actually be considered a 'conflict'?

'Cyberattack', however, is a very precise term. It indicates that some sort of action of an aggressive nature has occurred. At the same time, the word indicates that something has been attacked in a very literal sense, and since we are in cyberspace, that attack would have to be on parts of the digital infrastructure (or on physical infrastructure as a consequence of attack on digital infrastructure). In most cases, aggressive actions in cyberspace result in some sort of *breach*. To access an individual's personally identifiable information (PII), cybercriminals with enrichment motives must either breach the security measures in place on the individual's networked device or of a database in which the PII is stored, operated by a third party. Cyberactivism, aka hacktivism, also requires breach of security (the latter synonym is self-explanatory in this sense), as does cybervandalism. Breaches in any sense usually happen as a result of an attack of some sort. It also seems intuitive that cyberterrorism and cyberwarfare would involve some sort of attack.

Thus, I find the word 'cyberattack' to be the most fitting term for the kind of activity which would constitute the unit to be classified in the above five categories. Nguyen (2013) also seems to prefer this term, and she has observed two general uses of the term, the object-based definition and the instrument-based definition. The first defines a cyberattack by the object under attack, the second by the instrument utilized in the cyberattack. She argues that the object-based definition as used by a number of scholars and US governmental institutions is not just too broad, it is also a hindrance to more extensive and technologically contemporary legislation. She finds that the object-based definition is problematic because "Although computers can be, and often are used to execute attacks targeting other computers, bombs can also destroy computer facilities or transmission lines, and electromagnetic pulse energy can be manipulated to overwhelm computer circuitry or jam communications" (p. 1087). With this definition, Nguyen argues, cyberattacks cannot legally be distinguished from 'kinetic' attacks, which she states is the most widely used term for (often military) attacks on non-digital infrastructure or objects.

This is problematic because it leaves no room for the cyberspace-specific properties of cyberattacks, such as the attribution problem or the simultaneous acquiring of information as well as damaging infrastructure. Furthermore, "Computers and computer networks hold no special legal status relative to other potential targets for destruction, so a missile strike against a computer facility poses no difficult question for international law" (p. 1087), which Nguyen finds problematic since there is clear empirical evidence of legislative difficulties related to international cyberattacks. Instead, Nguyen suggests that the instrument-based definition is used. Here, it is not the object that is 'cyber', but rather the instrument used in the attack. This definition of 'cyberattack' can cover both kinetic and digital targets, as long as the attack is performed with some sort of computing device.

This, Nguyen writes, is also in accordance with other military or law enforcement vernacular, e.g., 'air attack' or 'amphibious assault'. Crucially for Nguyen, it also makes it more manageable to use the term 'cyberattack' in a *jus ad bellum* (i.e., the justification for war or just preparation for war) context: "The language of jus ad bellum relies upon concepts such as scope, duration, and intensity in speaking of the use of force, armed attack, and aggression. These are all concepts bearing more on the type of force exerted against a target than the character of the target attacked" (p. 1089). Following Nguyen's arguments, I have chosen to adopt the instrument-based definition of the term.

We can now begin to see the contours of a taxonomy of cybersecurity. In Fig. 2 I have illustrated the relationship between the different categories mentioned above, and how they each represent a type of attempt to compromise cybersecurity. The table in Fig. 2 also contains some attributes that distinguish the categories from each other, such as whether a kinetic attack could follow from the cyberattack ("Kinetic crossover"), which type of actors are behind the attack, the typical objective of the attacks, and whether international or local law is applicable.

		Cyberattack Categories			
	Cyberterrorism	**Cybercrime**	**Cyberactivism** **Cybervandalism***	**Cyberwarfare**	**Cyberespionage**
Spheres	Public, Private, Internal, Authority	Private, Internal	Public, Private, Authority	Public, Private, Internal, Authority	Public, Private, Internal, Authority
Actors	NSAs	NSAs (SA rare)	NSAs	SAs, NSAs	SAs, NSAs
Kinetic crossover	Yes	Yes	Rare	Yes	No
Objective	Fear / damage	Financial / Info acq.	Political / Info acq./Damage	Damage/deterrence/ Info acq.	Financial/Political/ Info acq.
Law	Local	Local	Local	International	Local

Fig. 2. Cyberattack categorization. (NSAs=Non-State Actors, SAs=State Actors). *=Note that these two terms are not conflatable, but merely share the same properties in this particular regard.

These properties are all quite speculative, as further research is required in order determine the prevalence of each property within the category. This could be in the form of a study of all recent cyberattacks of a certain scale with statistical analyses of the incidence of each property, but has not been possible within the timeframe of preparing this paper. Instead, the above properties are based on a small amount of empirical evidence, observed by the author over time.

Cyberattack actors and places

In Fig. 2, I have added a 'Spheres' property in order to illustrate which domain the attack happens in, and who the targets/victims are. The division of society into different spheres comes from Habermas, who suggests at least four spheres: internal (intimsphäre, the personal), private sphere (civil society, corporations), public sphere (organizations and the public discourse), sphere of public authority (national institutions, governments/states) (Habermas, 1989). Habermas presents these in *The Structural Transformation of the Public Sphere* through a neo-marxian, historical description of the emergence of the public sphere (*Öffentlichkeit)* in the bourgoisie of pre-industrial Europe. It is important to note that Thomas McCarthy's 1989 English version of the book that is referenced here translates the term *Intimsphäre* as "interior domain" and "internal space" (Habermas 1989 p. 30). From the English version, it would appear tha Habermas only identifies three spheres. The literal translation of *Intimsphäre*, however, is "intimate sphere". Thus, in its original German, *The Structural Transformation of the Public Sphere* presents four spheres: *Intimsphäre*, *Privatsphäre*, *Öffentlichen Sphäre*, and *Staatliche Sphäre*, which correspond to the spheres in the list mentioned above. These spheres, along with other spheres such as the sphere of political communication, sphere of public assembly and sphere of private autonomy, are divided into two realms, public and private.

Using Habermas' spheres provides a simple way of illustrating the nature of the victims of a cyberattack. In order to understand this classification, I have provided a non-exclusive list (Fig. 3) of attackers and targets in cyberattacks that fall into these four classes.

Targets	Attackers
Individuals	Individual Black Hat hackers
Nation States / Critical Infrastructure	Nation States/state-employed hackers
State agencies / Military	State agencies, usually security agencies
Non-Profits and NGOs	Autonomous/Non-State hacker groups
White hat hackers and security experts	Hacktivists
Corporations	Cyberspies
Research facilities and universities	Cybercriminals with enrichment motives

Fig. 3: List of actors and attackers in cyberattacks (Source: Maisey, 2014).

This leads us to a more specific review of where cyberattacks happen. To use an analogy from traditional law enforcement and military language, the attacks happen in many different battle zones and crime scenes, and I shall now attempt to describe these, using Habermas' spheres as a guideline.

Internal sphere

This is the domain of personal computing devices which can be targeted for cyberattacks. These include, but are not limited to, personal computers, personal computer peripherals and accessories,

feature- and smartphones, tablets, phone/tablet combinations (phablets), set-top-boxes, game consoles, routers, modems, home automation devices and more. These devices are usually connected to some sort of network – most likely the Internet – and are therefore exposed to cyberattacks. Many of them contain, or can lead to PII, which can then be used in cybercrime for enrichment purposes or surveillance contexts. It is estimated that PII was retrieved from the devices of 187 million people the world over in 2011 (Hiller & Russell, 2013). Sicari et al. (2015) point to the increasing number of home and personal devices that become connected (popularly known as the Internet of Things [IoT]), such as smartwatches, cars, kitchen and bathroom devices, door locks and home automation systems, as a serious problem. They argue that current cybersecurity systems at the personal level are not scalable enough to be able to withstand the cyberattack onslaught which might happen because the more devices are online, the higher the chances are of the emergence or existence of vulnerabilities. (Sicari et al., 2015). The authors suggest changes to the flexibility levels of cybersecurity infrastructures.

Private sphere

In the private sphere, we find mostly attacks of a corporate nature. These can cross over into the Internal sphere, however. Examples of this include attacks on corporation/third-party databases in which PII about individuals is stolen. Recent examples include the Target, Home Depot, Sony and Anthem attacks.

But the private sphere is also home to cyberattacks performed with corporate cyberespionage motivations. Moore (2010) documents how 21 Israeli company executives had hired private investigators to install spyware on competitors' computers, how Chinese spies were systematically targeting UK businesses, and how a survey of 800 CIOs revealed a majority who believed their company had been under attack with losses of an average of $4.7 million annually. Nation-state attacks on corporations are also widespread, but depending on the motivation and damage done, they can actually also constitute cyberwarfare rather than cyberespionage or cybercrime**.**

Public sphere

The media, as a venue for production and presentation of discourse, plays a large role in Habermas' public sphere. Cyberattacks on media outlets are common, with notable examples including attacks on The New York Times, The Washington Post and The Wall Street Journal (Reuters, 2013), and the Syrian Electronic Army hacking into the Associated Press' Twitter account to tweet out a false tweet about the president being wounded in a bomb attack on The White House. (Fisher, 2013). But Habermas' public sphere also refers to other venues of discourse production. Non-profit organizations and NGOs are also under constant attack, which in themselves constitute cyberattacks in the public sphere (Maisey 2014). But more importantly, it is in the public sphere we find one of the cyberattack targets which provokes the most fear: attacks on collectively-owned and distributed physical, critical infrastructure such as power plants, electricity grids, railways and SCADA (Supervisory Control and Data Acquisition) systems. The latter are systems which uses communication networks to control large installations in critical infrastructure. That this is a serious threat is shown by Hiller and Russell (2013), in which it is stated that an estimated 25% of all power companies globally have experienced cyberattacks.

Public authority sphere

In this sphere, we find nation-state actors as both targets and aggressors, and as a natural consequence, the categories cyberterrorism, cyberespionage and cyberwarfare are all present here. Two particularly

problematic issues in this sphere is the problem of attribution (Tsagourias, 2012; Hare, 2012), which is one of the biggest differentiators distinguishing cyberwarfare from traditional warfare, and the implication of both state actors and non-state actors in conflicts and cyberterror attacks (Sigholm, 2013). In cyberwarfare, non-state actors can be both targets and aggressors in a type of conflict which traditionally has only had nation-states as participants. The wires are crossed in cyberwarfare, as non-state actors in the shape of individuals or hacker groups can engage in political support attacks without having formal or practical ties to the state they support. Nation-states can also attack private corporations and individuals to serve a military purpose and to gather information – something that is challenged by conventions and treaties in traditional warfare. All of these subjects are explored later in this proposal.

TOWARDS A DEFINITION OF CYBERSECURITY

As evidenced by the discussion above, a very precise definition of the term cybersecurity that can be summed up in a few sentences seems quite elusive. However, a few conclusions can be drawn which are helpful in the journey towards a workable *interpretation* of the term:

- Cybersecurity is a security matter, i.e., it is concerned with freedom from threats.
- Threats to cybersecurity all share the common trait that they constitute the threat of a breach/attack.
- Cybersecurity, although related, is different than information security and computer security.
- From the definitions put forward by Craigen, Diakun-Thibault and Purse (2014), DHS (2015) and ISO (2012), there is a clear tendency towards defining cybersecurity as primarily being concerned with the security of systems, rather than individuals. When looking at these systemic definitions through the lens of security studies, they seem to fall into the traditional category.
- Critical security studies offers a different perspective on the concept of security, with particularly the Aberystwyth and Copenhagen schools introducing both the individual and the discourse into security analysis. Critical security studies also opens up security studies to analysis of other types of security, e.g environmental security or, relevant to this text, cybersecurity.
- There seems to be a shortage of literature which employs critical security studies in order to understand cybersecurity.
- A working definition of cybersecurity must address that which the referent object is being secured against, i.e., the threats to security.
- In the case of cybersecurity, there are several types of threats, but what they all have in common is that they entail some sort of digital breach/attack.
- If one adopts a materialist view on the digital, such a breach/attack compromises physical security measures comparable to the physical damage inflicted by the threats dealt with in

security studies writ large (albeit on a micro-level). This is augmented by the existence of 'kinetic crossover' events, in which a threat to cybersecurity crosses over to become a threat in the non-digital space.

CONCLUSION

Above, I have explored the different theoretical and interpretational aspects that could or even should be considered when discussing cybersecurity as a concept and a term. Through application of theory from critical security studies as well as philosophy and sociology, I have shown that cybersecurity as a concept inhabits a space which is bigger than simply protecting computers from viruses or hacker attacks. Cybersecurity is a security matter which spans from the individual's security against cyber threats to all of society. As such, the concept of cybersecurity demands a multi-faceted theoretical approach, which I have attempted to show above. In conclusion, however, we are left with a definition of cybersecurity that is anything but specific, and is open for even more research and theorization in the future.

REFERENCES

Archives.org (2015). The Constitution of the United States: A

Transcription.Available at http://www.archives.gov/exhibits/charters/constitution_transcript.html

Ayoob, M. (1997). Defining security: a subaltern realist perspective. In *Critical Security Studies*. University Of Minnesota Press.

Bigo, D., Tsoukala, A., & Lecturer, S. (2008). Terror, Insecurity and Liberty. *International Relations*.

Bishop, M. (2003). What is computer security? *Security & Privacy, IEEE,* 1(1), 67–69.

Bishop, M. (2005). *Introduction to computer security (1st ed.).* Boston, MA: Pearson Education.

Blanchette, J. F. (2011). A material history of bits. *Journal of the American Society for Information Science and Technology*, 62(6), 1042–1057.

Borgman, C. (2007). *Scholarship in the Digital Age*. Cambridge, Mass.: The MIT Press.

Bowker, G. (1993). How to be Universal: Some Cybernetic Strategies, 1943-70. *Social Studies of Science*, 23(1), 107–127.

Bowker, G. C. (2008). *Memory Practices in the Sciences.* MIT Press.

Buzan, B. (1991). *People, States and Fear: An Agenda for International security studies in the Post Cold War Era.* Colchester: ECPR Press.

Buzan, B., & Hansen, L. (2009). The Evolution of International security studies. *Political Science.*

Cavelty, M. D. (2012). Cyber-security. *Contemporary Security Studies*, 1–33.

Clynes, M., & Kline, N. (1960). Cyborgs and space. *Astronautics.* September. 26–27, 74–75.

Connelly, P.J. (2015) John Locke. *Internet Encyclopedia of Philosophy*. Available at

http://www.iep.utm.edu/locke/.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cyber-security. *Technology Innovation Management Review*, (October), 13–21.

Denning, D. E. (2012). Stuxnet: What Has Changed? *Future Internet*. DHS. (2015). Explore Terms: A Glossary of Common Cybersecurity Terminology.

Retrieved January 1, 2015 from http://niccs.us-cert.gov/glossary

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, 28(3-4), 189–198.

Dostal, J. M. (2004). Campaigning on expertise: how the OECD framed EU welfare and labour market policies–and why success could trigger failure. *Journal of European Public Policy*, *11*(3), 440-460.

Enloe, C. (1989). *Bananas, Bases and Beaches: making feminist sense of international politics*. London: Pandora.

Enloe, C. H. (2000). *Maneuvers: The international politics of militarizing women's lives.* University of California Press.

European Commission. (2014). Fact sheet on the "Right to be forgotten Ruling". Brussels. Available at: http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf

Fisher, M (2013). Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism? *The Washington Post.* Available at

https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/

Ganguly, S. (2015). *The Snowden Reader*. D. P. Fidler (Ed.). Indiana University Press.

Geoghegan, B. D. (2008). The historiographic conceptualization of information: A critical survey.*IEEE Annals of the History of Computing*, 30(1), 66–81.

Gibson, W. (1982, July). Burning Chrome. *Omni*.

Gibson, W. (1984). *Neuromancer*. New York: Ace.

Glass, L., & Gresko, R. (2012). Legislation and Privacy across Borders. 2012

International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing.

Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. Cambridge, MA: MIT Press.

Habermas, J. (1990). *Moral consciousness and communicative action*. Cambridge, MA: MIT Press.

Habermas, J. (1994). *Justification and application: Remarks on discourse ethics*. Cambridge, MA: MIT Press.

Haraway, D. (1991). A cyborg manifesto: science, technology, and socialist-feminism in the late twentieth century. In *Simians, cyborgs and women: The reinvention of nature* (pp. 149–181). Routledge.

Hayles, N. K. (1999). How we became posthuman: Virtual bodies in cybernetics, literature and informatics. *Journal of Artificial Societies and Social Simulation* (Vol. 4). University of Chicago Press.

Herz, J. H. (1951). *Political realism and political idealism*. Chicago, IL: University of Chicago Press.

Holloway, D. (1974). Innovation in Science--the Case of Cybernetics in the Soviet Union. *Social Studies of Science*, 4(4), 299–337.

Hopf, T. (1998). The Promise of Constructivism in International Relations Theory. *International Security*, 23(1), 171–200.

ISO/IEC. (2012). ISO 27032 *Information technology - Security techniques - Guidelines for cybersecurity*. International Organization for Standardization.

ISO/IEC. (2014). ISO 27000 *Information technology — Security techniques — Information security management systems — Overview and vocabulary* (Vol. 2014). International Standards Organization.

Kang, M. and Jang, J. (2013), NIMBY or NIABY? Who defines a policy problem and why: Analysis of framing in radioactive waste disposal facility placement in South Korea. *Asia Pacific Viewpoint*, 54: 49–60.

Leary, T. (1988). The Cyber- punk : The Individual as Reality Pilot. *Mississippi Review*, 16(2),252-265.

Lehtinen, R. (2006). *Computer security basics*. O'Reilly. Retrieved from http://oreilly.com/catalog/9780937175712

Merriam-Webster. (n.d.). Entry: "Cybersecurity." Retrieved January 1, 2015, from http://www.merriam-webster.com/dictionary/cybersecurity

Morgenthau, H. (1948). *Politics Among Nations*.

Newitz, A. (2013). The bizarre evolution of the word "cyber." Retrieved from http://io9.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487

Nguyen, R. (2013). Navigating jus ad bellum in the age of cyber warfare. *California Law Review.*

Niebuhr, R. (1952). *The Irony of American History*. Charles Scribner's Sons.

Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and implications. *ICIW*, 267–270.

Peoples, C., & Vaughan-Williams, N. (2015). *Critical security studies*.

Peters, B., & Geoghegan, B. D. (2014). Cybernetics. In M.-L. Ryan, B. Peterson, & L.

Emerson (Eds.), *The Johns Hopkins Guide to Digital Media* (pp. 109–111). Baltimore, MD: Johns Hopkins University Press.

Public Safety Canada. Emergency Management Vocabulary (2012). Retrieved from http://www.bt-tb.tpsgc-pwgsc.gc.ca/publications/documents/urgence-emergency.pdf

Reuters (2013) *Cyber attacks against media on the rise, rights group says* Available at: /www.reuters.com/article/2013/02/14/net-us-media-cyberattacks idUSBRE91D1LN20130214#ZHThd34bLzRxlO62.99

Richardson, J. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. *Global Investment Watch*.

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and

trust in internet of things: The road ahead. *Computer Networks*, 76, 146–164. Talbot, E. B., Frincke, D., & Bishop, M. (2010). Demythifying cybersecurity. IEEE *Security and Privacy*, 8, 56–59.

Tan, L., & Wang, N. (2010). Future internet: The Internet of Things. In 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE) (Vol. 5, pp. 376–380).

Tatar, Ü., & Çelik, M. M. (2015). Hacktivism as an emerging cyberthreat in *Terrorism online: Politics, law and technology*, 54.

Tickner, J. A. (1992). *Gender in international relations: Feminist perspectives on achieving global security*. Columbia University Press.

Umpleby, S. (2000). Defining "Cybernetics." Retrieved from http://www.asc-cybernetics.org/foundations/definitions.htm

Vinge, V. (1981). True Names. *Binary Star*, (#5).

Von Solms, R., & van Niekerk, J. (2013). From information security to cybersecurity.

Computers & Security, 38, 97–102.
Wæver, O. (1990). The Language of Foreign Policy. *Journal of Peace Research*, 27(3), 335–343.

Wæver, O. (1995). Securitization and Desecuritization. In R. D. Lipschutz (Ed.), *On security* (pp. 46–76). Cambiridge University Press.

Wæver, O. (2004). Aberystwyth, Paris, Copenhagen: New "schools" in security theory and their origins between core and periphery. *Security Studies*. Retrieved from http://bespo.org/upload/93a145a3a12b1b8aa2e33c1ebd320d91.pdf

Waltz, K. (1979). *Theory of International Politics.* New York NY: McGraw-Hill.

Weldes, J., Laffey, M., Gusterson, H., & Duvall, R. (1999). Introduction: constructing insecurity. In *Cultures of insecurity: States, communities and the production of danger* (pp. 1–33). Univ Of Minnesota Press.

White House, the. (2015). FACT SHEET: White House Summit on Cybersecurity and Consumer Protection. Press Release, available at https://www.whitehouse.gov/the-press-office/2015/02/13/fact-sheet-white-house-summit-cybersecurity-and-consumer-protection

Wiener, N. (1948). *Cybernetics, or control and communication in the animal and the machine.* Paris: Hermann.

Wiener, N. (1956) *I am a mathematician*. New York: Doubleday.

Zimmer, B. (2013). "Cyber" Dons A Uniform. Retrieved January 1, 2015, from http://www.wsj.com/articles/SB10001424127887323419604578569993261826614