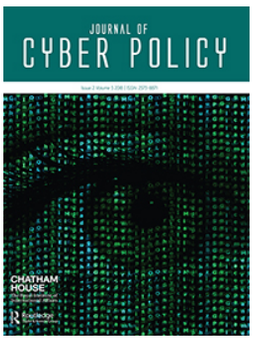

Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

'Cyber' semantics: why we should retire the latest buzzword in security studies

Andrew Futter

To cite this article: Andrew Futter (2018) 'Cyber' semantics: why we should retire the latest buzzword in security studies, Journal of Cyber Policy, 3:2, 201-216, DOI: 10.1080/23738871.2018.1514417

To link to this article: https://doi.org/10.1080/23738871.2018.1514417

Published online: 30 Aug 2018.

JOURNAL OF CYBER POLICY
2018, VOL. 3, NO. 2, 201–216
https://doi.org/10.1080/23738871.2018.1514417

Routledge
Taylor & Francis Group

'Cyber' semantics: why we should retire the latest buzzword in security studies

Andrew Futter

Department of Politics & International Relations, University of Leicester, Leicester, UK

ABSTRACT

The word 'cyber' has become one of the most ubiquitous and powerful concepts in contemporary security studies. Very few academic papers or workshops in the social sciences fail to touch upon the 'cyber challenge' in some way, and very few politicians fail to use the term when talking about the most pressing threats to national security. But surprisingly, little consensus exists about what the term includes, refers to, or how it is being used differently by different people in different contexts. Indeed, there is no single definition or research agenda that all adhere to. This in turn often drives hype and leads to misunderstanding and bad policy. The result is that formulating suitable policies to deal with and respond to threats to digital computers and networks, either domestically or internationally, has become disjointed and obfuscated, with straw-man arguments based on erroneous assumptions often prevailing. This paper unpacks and explains these problems, before making the case for jettisoning the word 'cyber' from the security studies lexicon and returning instead to the language first developed by computer science in the 1990s. Only by doing this can we properly begin to understand, manage and mitigate the security challenges of the latest information age.

ARTICLE HISTORY
Received 11 January 2018
Revised 3 August 2018
Accepted 8 August 2018

KEYWORDS
Cyber; cybersecurity; cyberwar; computer network operations; information security; information warfare; computer science

Introduction: why using the word 'cyber' in security studies is a problem

In a 2016 televised presidential debate with Hilary Clinton, then Republican nominee Donald Trump was quoted as saying that 'the cyber' was one of the biggest threats facing the United States, and that the U.S. must 'get very, very tough on cyber' (quoted in Lafrance 2016). While President Trump is certainly not the only person to use the concept as a noun (Wolff 2016), it is indicative of a much broader problem when it comes to the word 'cyber', even when it is used as an adjective or a prefix. This is because over the past decade 'cyber' has come to refer to all manner of activities and threats, weapons and maybe even warfare involving computers, coding, networks and complex digital systems. Most nations now devote considerable resources to what they call 'cyberdefence' and 'cybersecurity', and in some cases, have developed offensive 'cyber' capabilities and units within their militaries. Indeed, the notion of 'cyberthreats' is increasingly impacting every part of military and security planning and the literature, hype and speculation surrounding this new concept has grown exponentially (e.g. Panetta 2012).[1] The result is that it has become popular to see

the word 'cyber' as representing one of the greatest security challenges of the modern era and possibly even a transformation in the contemporary security environment.

However, while the literature on 'cyber' has flourished, an accepted definition of the term – and therefore an agreement about its meaning, scope, nature and how it should be used – has yet to be decided. The phrase has become something of a catchall, whose meaning is often divined largely at the behest of the user or author and is often highly dependent upon the purpose or argument being made. Thus, many opinions, statements, studies and policy prescriptions regarding threats to computers, networks and digital systems lack a clear understanding of what the concept means and what it involves. Different scholars, practitioners and even states treat and understand the term differently, conflating very distinctive and often conflicting meanings, and therefore exacerbating and clouding problems and concerns rather than helping to resolve them.[2] The meaning of 'cyber' and the 'cyberthreat' therefore often remains very much in the eye of the beholder, and the inability to be clear what the concept means, involves and affects has left the word dangerously devoid of meaning, and has obfuscated and complicated the ability to shape suitable responses and policies.[3]

What therefore seems apparent is that the language being used to describe the new security challenges posed to computer systems and networks by hackers, digital coding, malware and other technologies is making it more rather than less difficult to understand and respond to a new security landscape. 'Cyber' may be a buzzword, albeit with some value in day-to-day use or as a very general descriptor, but in academic security studies and policymaking it has become so nebulous that it has essentially become meaningless; it simply refers to too many different things at different times for different people. As such, this article makes the case for greater clarity and precision in the way that we talk about modern security threats, calls for a return to the language first developed by computer scientists in the 1990s, and argues that ultimately security studies and policymaking would be better off without the world 'cyber'.

This article proceeds in five sections, each of which provides a key reason why the 'cyber' moniker should be retired: (1) the first explains that a significant part of the problem is that the word 'cyber' began life with nothing to do with security studies, but became entangled with debates about information warfare, and slowly emerged as the catchall term that we know today in the 1990s; (2) the second explains that because seeking a single definition of 'cyber' has proved impossible, and because no accepted research agenda exists, the result has been confusing, hamstrung and unproductive debates; (3) the third shows the problems that have been caused by using the phrase 'cyber' to refer to such a wide gamut of threats with considerable differences in their nature, scope and implications; (4) the fourth shows that the use of the word 'cyber' has been a major impediment to constructing political agreements because experts and officials are so often talking past each other or misunderstand the nature of the challenge due to the vocabulary being used; (5) the fifth argues that the best thing for security studies and policymakers is to return to the language first developed a generation ago, principally by those in the hard sciences and military organisations, and to jettison the 'cyber' moniker altogether. Finally, the conclusion explains why an academic and policy world characterised by far more linguistic clarity, precision and acceptance is the only way to properly begin to understand, conceptualise and mitigate the most pressing security challenges of the current information and digital age.

'Cyber' originally had nothing to do with security studies, but became a popular catchall term in the 1990s

The first reason why it makes sense to retire the word 'cyber' from security studies and policymaking is because it was never intended to be used for this purpose, and once it became part of the academic and political lexicon in the mid-1990s, came to represent so-many different dynamics that it became hollow and increasingly nebulous. As to why this word came to dominate modern academic and policy debates is an interesting question, but the fact that it did, and the fact that it came to mean so many different things to different people, is a key reason for the failure of scholars and policymakers alike to seriously engage with the myriad challenges that the word encapsulates.

The etymology of the word 'cyber' can be traced back to Ancient Greece and the phrase *Kybernetes* – which translates roughly as 'helmsman' or 'the art of steering' (Tabansky 2011, 76). The word as we know it didn't emerge until the 1940s and the publication of *Cybernetics* by the American mathematician Norbert Wiener (1948): *Cybernetics* was a study of the importance of systems in both living beings and artificial machines. The term then became popularised in the 1980s as part of the 'cyberpunk'[4] movement, and most notably in the novel *Neuromancer* by science fiction writer William Gibson (1984). By the end of the 1980s the word 'cyber' thus became associated with popular culture and a particular style of futuristic, dystopian writing. But at around the same time as the emergence of the cyberpunk movement, there was a recognition in U.S. military circles that the latest information age, and especially the advent and spread of sophisticated computers for military operations, was changing the modern battlefield and opening up new possible avenues for warfare. The result was the development of Information Warfare (IW) or Information Operations (IO), and the associated Revolution in Military Affairs (RMA) (Collins and Futter 2015). As Ben Zimmer put it 'cybersex and cyberwar "grew up side by side"' (quoted in Newitz 2013).

While information has always been central to warfare, the ability to target complex computers, digital networks, the electromagnetic spectrum, and real-time media as part of the latest information revolution,[5] allowed IW/IO to blossom as a specific field of military activity and strategy (although its antecedents can probably be traced back to the 1970s [Berkowitz and Han 2009]). IW/IO are multifaceted concepts covering many different activities, including sabotage, espionage and intelligence operations, telecommunications eavesdropping and fraud, psychological operations, perception management and Electronic Warfare (EW) (Denning 1999, xii). Perhaps most importantly, new modes of IW/IO would now include what was termed Computer Network Operations (CNO), that is operations conducted through digital networks and against computers used to store and process information and that facilitate ever-more complex military weapons systems.

What seems to have happened sometime in the mid-1990s is that the label Computer Network Operations – which referred to a very specific set of capabilities and actions-was increasingly replaced with the word 'cyber' in the popular discourse. This may have had something to do with the publication of the seminal article 'Cyber war is coming!' by John Arquilla and David Ronfeldt in the academic journal *Comparative Strategy* in 1993. Two years later, an inter-agency task force investigating the weaknesses of U.S. critical national infrastructure needed a phrase to capture the challenges posed by new computer vulnerabilities within these systems, and the word they chose was 'cyber' (Kaplan 2016,

45–46).[6] Since then, the 'cyber' label appears to have come to replace IO/IW and refer to far more than CNO (especially in Western discourse). This is probably because new computer technologies were transforming each of the other aspects of IW/IO as well as providing a new niche CNO capability. This is particularly notable for Electronic Warfare (EW) (Anderson 2008, 568), where new digital capabilities drove a shift in IW and EW to targeting digital rather than analogue systems; and from primarily intercepting or disrupting information flows, to being able to alter, corrupt or delete that information (Kaplan 2016, 4–5).

But it also meant that the term was becoming diluted and increasingly ill-defined and was a key reason why it has come to be seen today as including such a broad range of factors. The phrase 'cyber' consequently went from referring primarily to Computer Network Operations as a component of Information Warfare, to something that also captured the transformation in each of the other aspects and subsets of IW as well, such as psychological operations, intelligence warfare, perception management and particularly electronic forms of exploitation and attack (Libicki 2007, 16–17). It was no coincidence that the language of IW, IO and CNO had begun to disappear from the forefront of the academic debate by the early 2000s, only to be replaced by the 'cyber' moniker as the go-to concept for discussing and analysing the security challenges of the latest information age.

Despite deriving from mathematics and science fiction, by the 1990s the word 'cyber' had become the go-to descriptor for a range of dynamics and threats that appeared synonymous with the computer age. Whatever the reason was for this – and it could be something as simple as the attractiveness of the word in popular culture – it meant that 'cyber' came to refer to a very broad range of quite different things; it also meant that 'cyber' replaced the more precise language developed at the start of the 1990s. For the next two decades, more and more activities, phenomena and dynamics would be labelled as 'cyber', especially in the social sciences, to the point where scholars, analysts and policymakers were often talking past each other and the concept had essentially become meaningless. This complicated evolution is almost certainly why we have such confusion over the use of the term today.

Producing an agreed definition of 'cyber' and a suitable research agenda has so far proved impossible

The second reason that the word 'cyber' should be retired is because there is no one definition that all adhere to when using the term, which in turn has confused the 'cyber debate', if such a thing can be said to exist. This is a direct product of the disjointed evolution of the concept and how it has been used (as discussed above), but it is also because different experts and officials have different conceptualisations about what the concept and debate should focus on. More problematically, it is often not clear what type of framework or understanding is being used, and therefore where the 'cyber' research agenda is and should focus.

There is no one accepted definition or conception that all adhere to when using the phrase 'cyber' or 'cyberthreat' (Owens, Dam, and Lin 2009, 14–15). In fact, use of the term spans a wide variety of different areas and scenarios, and incorporates a plethora of different referents and phenomena (Rattray 2001, 8–9). The Glossary of the Tallinn Manual produced by the NATO Cooperative Cyber Defence Centre of Excellence, which

is generally seen as one of the best attempts to agree definitions in this realm, describes the word 'cyber' as 'Connotes a relationship with information technology' (Schmitt 2013, 258).[7] But this is inherently vague and could mean many things. Likewise, the Oxford English Dictionary, which describes it as: 'Relating to or characteristic of the culture of computers, information technology, and virtual reality.'[8] Understanding and uses of the term can therefore range between very narrow and discrete conceptions and much broader inclusive frameworks (Rattray 2001, 8–9). This holds true at both the individual analytical level as well as at the strategic level, where Russia and China tend to prefer the label 'information' (Lewis 2011), and a far broader conception of information-based attacks, as opposed to the perhaps more discrete U.S. and Western preference for the term 'cyber' as (what would previously have been called) Computer Network Operations (Giles and Hagestad 2013). Consequently, for Russia and China, Information Warfare or 'cyberattacks' would include political actions designed to destabilise governments as well as more discrete CNOs.

At the heart of the problem is the fact that the 'cyber' label is often used-sometimes simultaneously-to describe: (i) the digitised real-time *context* within which we all live and operate, and a 'cyber' information or digital age; (ii) a *domain* of military operations – or as Daniel Kuehl conceptualises it, 'global domain' (2009, 28) which includes both physical and logical components, and which might be seen as being synonymous with the word 'cyberspace' (although this phrase is by no means unproblematic either); and (iii) a set of new *capabilities* and tools that can be used against computers and networks (the closest to the original category of CNO). Each of these understandings of the term have a different set of central questions and referents, and all apart from the narrowest CNO-based conceptualisations (or 'cyber' as discrete tools) might include both physical and non-physical aspects of the electromagnetic spectrum, as well as machines and people, and particularly the human–computer interface (Kramer 2009, 6; Kuehl 2009, 28). This means that there is no established academic research framework or clear policy focus to the debate.

It is therefore unclear what exactly 'cyber' analysis, studies or policy should focus on. One can think of at least four levels of analysis that might fall under the 'cyber' moniker depending upon conceptualisation and definition: physical/mechanical, logical, informational and human/cognitive (Rattray 2001, 17–18; Kello 2013, 18; Futter 2016, 6–9). (i) The first, *mechanical*, involves physical infrastructure and hardware such as wires, computers, communications nodes and mainframes that permit the creation, circulation and storage of information. (ii) The second involves the *logical* domain that includes the commands that tell the hardware what to do and the software that allows the transmission, interpretation and sharing of key information. (iii) The third is the *information* and data that the system collects, stores, generates and relies upon to function. (iv) The fourth is the cognitive domain, and specifically, *human* beings and their interaction with the hardware, software and information. Each of these aspects could be legitimately included as part of any study or analysis of 'cyber' challenges or threats and would provide very different conclusions and recommendations. Moreover, an operation labelled as 'cyber' could of course span more than one of these domains: for example, as Jason Andress and Steve Winterfeld point out, 'physical attacks can have logical effects and logical attacks can have physical effects' (2011, 120). Consequently, the *nature* of an operation

or challenge (i.e. the capability being employed) is often confused or commingled with the intended *effect* or *target* (i.e. a particular system or process).

The failure to agree an accepted academic or policy definition of 'cyber', and the inability to formulate a clear agenda for enquiry and discussion, has meant that many voices in the 'cyber' debate either talk past each other or are misconstrued. The language and vocabulary being used is fundamental to unpacking what exactly is being analysed or discussed, and of course, what this means for the broader suite of challenges being examined. Clearly, those that view 'cyber' as discrete CNO are likely to have a very different agenda, debate, and theoretical and policy implications than those that view the term as referring to a new domain of operations, and especially those who see it as a broader societal dynamic that impacts everything that we do.

The phrase 'cyber threat' is used to refer to very different things, with very different implications

The third reason that the 'cyber' label has served to obfuscate rather than improve our understanding of modern security challenges is because it is used to cover such a wide and differentiated variety of threats. Notwithstanding the fact that 'cyberthreat' can often be used to refer to problems that are inherent within computer systems, coding and networks-so called 'bugs'[9] that can cause a system to go wrong or act differently to what is intended without any outside interference, it also covers such a variety of activities that again the phrase can become problematic. Each instance or type of hacking or malware raises different questions and represents very different types of threats, but these are too often grouped together as one. This has prevented better academic discussion of the challenge as well as inhibiting a more concerted policy debate. To date, the clear majority of 'cyber' operations have been designed to cause nuisance, test systems, steal information and perhaps discover new vulnerabilities, rather than to implant highly sophisticated malware into sensitive machines and systems or to cause damage. But the language used in academic and political debates does not always reflect this, and the resulting hype is often bad for policy (Lee and Rid 2014). There are three major aspects of this problem that are worth noting.

First, the phrase 'cyberthreat' is used to refer to anything from simple hacking, hacktivism (the use of computers and networks to promote political ends), nuisance, vandalism and crime – which might be carried out by any type of actor and be of relatively minimal concern (other than to the victim of course), through denial of service and espionage, up to sabotage, destruction and possibly existential attacks or warfare, much more likely to be the preserve of powerful actors or nation states. As Thomas Rid and Peter McBurney explain, this 'cyber spectrum' ranges considerably in terms of the nature of the threat, and runs from 'generic but low potential tools, to specific but high potential weaponry' (2012, 8). This also impacts the type of actors likely to be involved. Generally speaking, more sophisticated attacks are likely to be the preserve of the handful of states with very advanced Computer Network Operations capabilities (usually thought to include the United States, Russia, China, the U.K., and Israel). Less sophisticated 'attacks', crime[10] and nuisance are more likely to be perpetrated by criminals or small substate groups (McConnel 2009, 76). Because of this, complex, widespread and high-level operations against sensitive computers and networks are unlikely to be a weapon of the weak

(Lindsay 2013, 389), or necessarily the go-to option for terrorists (Weimann 2005; Giacomello 2010). That said, espionage and penetration testing is often a state-based activity, and it is at least possible that individuals or small groups could carry out a sophisticated operation in extraordinary circumstances.[11]

Second, there is an important difference between targeting data resident *inside* a system (e.g. sensitive or private information) or targeting the *processes* of that system (i.e. what it is intended to do). This was formerly seen as the difference between Computer Network Exploitation (CNE), or intelligence gathering activities and Computer Network Attack (CNA), which are actions that seek to destroy, disrupt or damage (Owens, Dam, and Lin 2009, 1). The conflation of the two in the 'cyber' discourse is yet another factor that leads to misunderstanding and threat-inflation (Ibid., 32), although exploitation might often be a precursor to attack, and because the delivery vehicles[12] for exploitation or attack can be very similar, or may even be the same, it can be difficult to distinguish between CNE and CNA in practice (Meyer 2011, 24). Either way, this – often inadvertent – misuse also serves to reify the notion that 'cyberattacks' are somehow homogenous, and that the use of 'cyber' capabilities could in some way be similar to a conventional military attack (Valeriano and Maness 2014, 349), which in the vast majority of instances simply isn't the case. Conventional bombs kill and maim people, destroy things and leave rubble; the majority of Computer Network Operations cause no physical damage at all, and no one has died as a direct result of an attack on computer systems.[13] This in turn complicates the debate about how to respond, and particularly about 'cyber deterrence', as is discussed later in this article. As a result, the phrase 'cyberattack' or CNO might often be better understood in the first instance as a statement of methodology rather than effect (Owens, Dam, and Lin 2009, 11).

Third, 'cyber threat' is used to refer to operations that target the information space *via* computer-enabled systems (for example, seeking to confuse or deceive through the use of social media such as Twitter), versus those operations that attack information *within* computer systems (which would be classified as CNO). This perhaps provides the clearest distinction between Information Warfare that *utilizes* computer-based technologies or networks to achieve its purpose, and Computer Network Operations that target computer systems directly. A good example of this distinction would be the hacking of the Israeli military twitter account in 2014, when the attackers (purportedly the Syrian Electronic Army) were able to post a false tweet declaring a huge radiation leak after a missile strike on the Dimona nuclear facility in the Negev Desert (Tadeo 2014). This episode clearly utilised modern attack vectors, and was labelled as a 'cyberattack', but its main intention was probably to mislead and to spark a crisis indirectly rather than to steal information or damage the system directly.

Thus, the idea that we can speak of a homogenous 'cyberthreat' is unhelpful because such a wide gamut of very different activities, risks and dynamics fall under this label. These threats clearly vary considerably in their nature, seriousness and implications and therefore require very different forms of response. Instead, the current use of the phrase often leads to the unhelpful perception that there might be a single one-size-fits all response. Once we unpack the 'cyberthreat' discourse it is clear that the language being used does not always help to convey the true meaning of what is being argued or analysed, and this in turn often leads to hype and worst-case scenario thinking

(and therefore bad policy) (Lee and Rid 2014), when the reality, and the policy responses are almost always far more nuanced.

The language of 'cyber' has made developing policy responses and frameworks harder rather than easier

The fourth reason it makes sense to jettison the 'cyber' moniker is because it has hindered rather than helped the policy debate and the possibility of developing international frameworks and cooperation to address emerging challenges and threats. The use of a single descriptor has driven the perception that one-size-fits all policy responses are possible and desirable when it comes to 'cyber', whereas in reality this simply cloaks the complexity of the policy challenge, leads to strawman arguments and Manichaean thinking, and often ignores the more mundane, but ultimately very significant policy responses available.[14] It has also created a view that 'cyber' risks must be addressed by national governments and large-scale policies. The way that we respond to the challenges of the digital age must be multifaceted and tailored to specific problems and dynamics; this in turn means being clear and precise in the language that we use.

There are a number of problems in the 'cyber' policy debate, but the main one seems to be that while the majority of 'cyberthreats' occur at the lower end of the threat spectrum and often don't require particularly sophisticated or expensive responses, the focus is often on the top end, and on those that do. The reality is that because the majority of operations that are commonly labelled 'cyber' take place at the lower end of the threat spectrum, and involve hacking, hacktivism, crime or vandalism – often but not always perpetrated by individuals and non-state actors – the majority of the response should be focussed on better computer and online 'hygiene', better practices and stricter security processes (Lewis 2011). This also means focussing on the human aspect. Humans are often the easiest method of 'getting in' to a system; it is often far less complicated to target people and operators (often through some type of social engineering[15]) than it is to breach systems digitally or through networks alone (Ablon 2015). A considerable number of security breaches might have been prevented or at least been minimised had institutions or employees followed proper security protocols, such as changing passwords, downloading regular security updates or patches, and not opening suspicious email attachments, etc., the best example being the extent of the WannaCry operation against, amongst others, the U.K. NHS (Graham 2017), which could purportedly have been limited had security updates been downloaded.

Better computer hygiene and processes could then be augmented with enhanced security and defence. Air gapping – that is, separating computer systems from unsecured networks and the wider internet, is probably the best example of this. However, better Computer Network Defences, firewalls, a decent anti-virus programme, and an active network defence capability (human or automated) are all clearly part of the response to the challenge too. Better hygiene, security and defence are therefore clearly most applicable to 'cyber' operations perpetrated by criminals, hacktivists, and those seeking to steal information. It might also help dissuade so-called 'cyberterrorism' (see Kenney 2015). Lastly, many CNE operations, especially IP theft and crime, are best dealt with by national law enforcement agencies and through traditional criminal channels.

Three so-called strawman arguments about the challenges of the latest information age are also worth debunking. First, because the word 'cyber' has been used to refer to such a broad range of activities it is often held that traditional deterrence is impossible in 'cyberspace' or against Computer Network Operations (Siegfried Hecker in Cirenza 2016). But this is to reduce the 'cyber' challenge to an either/or question, which it is not. Instead it is entirely contingent upon what and who is being deterred, and how (Nye 2016/2017, 68),[16] and whether the attribution of capabilities is possible. Some attacks against critical national infrastructure probably can be deterred in certain circumstances through the threat of retaliation, or at least because the would-be attacker does not want to run the risk of conducting such operations and being caught. This only applies to the most sophisticated operations against computer systems, whereas much less serious activities should be dealt with in other ways such as through law enforcement and criminal proceedings (and often not by the national government). For example, when the U.S. Defence Science Board recommended that some cyberattacks might be deterred by a nuclear response (2013), this clearly did not include everyday hackers, criminals or even espionage.

Second, the same thinking is often taken to mean that it is impossible to have meaningful arms control or international agreements in the digital realm. Again, because of the catch-all nature of the language, there seems to be a belief that an all-encompassing treaty or agreement is the answer, but this neither makes much sense nor is probably achievable. Arms control or other confidence building mechanisms might be possible in certain areas (such as with systems that control critical national infrastructure or hazardous materials) but may not-or at least may not be the best approach-in others (crime, for example[17]). The key is in the precision of what is being discussed and the agreement being sought. For example, it doesn't make much sense to try to ban a noun like 'cyber' or even 'cyberattacks' in general, but you might be able to prohibit certain types of Computer Network Attacks or operations against the most sensitive computer systems, or even limit the use of certain capabilities through moratoria (i.e. attacks on the systems used to control nuclear weapons) (see Futter 2018). Likewise, even agreements that are seen as successful in the 'cyber' realm such as the 'US–China cyber agreement' leave much open to interpretation because of the language used (Bate 2015).

Third, imprecision in the language being used often means that it isn't clear *who* should take responsibility for addressing the myriad threats posed by 'cyber'. Hyping and obfuscation can lead to the perception that the 'cyber' challenge can only be met by national governments, but the reality is again more nuanced. Generally speaking, responding to these challenges should be split between the individual (through their actions online and securing their personal information); companies and organisations (through adherence to good information security policies and training); law enforcement agencies (who should take the lead against criminal activities that utilise computers and networks); and national governments (who both create the climate for better security but are also responsible for protection and responses against high level threats). Unlike previous security threats such as a nuclear attack, addressing threats to computers, networks and information therefore requires a whole-of-society approach and a strategy with different levels of responsibility.

The final point here is that vagueness of language may also be used instrumentally by those who benefit most and who have a vested interest in continuing to muddy what

'cyber' really means. There is certainly an argument to be made that military officials and computer security companies have used imprecise language to help bolster budgets and business through nurturing a bleak and scary picture of the current information environment (Singel 2010; Lee and Rid 2014). While the challenges should not be underestimated, it is incumbent on scholars and policymakers alike to become familiar with the nuances of the threat, and to separate the everyday challenges of the digital age (which might have to be managed individually or by organisations) from new risks that are posed to national security (which should be managed by governments). The response to the challenges of the latest information revolution must therefore be nuanced.

A better and more precise language for the challenges of the digital age already exists

The final argument for removing the word 'cyber' from the security studies literature and policy debate is because a better, more precise language and vocabulary already exists. This is the terminology developed in the 1980s and early 1990s by Computer Scientists and experts in the military and technical world, which was then superseded by the all-conquering 'cyber' moniker, especially in the Social Sciences. Interestingly, some of this language, especially the phrase Computer Network Operations continues to be used in various military planning documents, but not at the more public level. For example, US Cyber Command, UK National Cyber Security Centre, and the Israeli National Cyber Security Authority all have CNO policies and doctrine, but this is conspicuous by its absence in much academic writing and policy discussion.

There are three different levels to the language that we need to return to, all of which have at times been described as 'cyber'. The principle distinction should be between activities that are best characterised as Information Warfare and those that are Computer Network Operations, whilst recognising that *CNO can be part of IW*. A good example of this might be the hack of the Democratic Party in 2016, which utilised CNO, specifically Computer Network Exploitation, to acquire personal information, but also as IW because the data was then used-purportedly-to influence U.S. politics. But it also means differentiating between actions that directly target computer systems and their data and processes, and activities that utilise digital technology indirectly – for example, in propaganda or perception management. This also includes ensuring clarity for activities such as jamming communications or radar which might be better characterised as Electronic Warfare (that is, action utilising the electronic spectrum but not seeking to implant or alter coding).

Second, within the field of Computer Network Operations we need to return to the distinction between Computer Network Attack and Computer Network Exploitation. The phrase 'attack' should only be used when the intention or effect is to cause disruption, or physical damage, and should not apply to actions that seek to steal information and data. This also means that only the most sophisticated and destructive CNAs would therefore qualify as using 'weapons' (Rid and McBurney 2012). The Stuxnet malware that was believed to have jumped the air gap and disrupted computer processes at the Iranian uranium enrichment plant at Natanz is perhaps the best example of a CNA (see Zetter 2014). Likewise, operations such as Moonlight Maze in 1999 where thousands of sensitive U.S. documents were stolen by Chinese hackers, or the huge breach of the U.S. Office of

Personnel Management beginning in 2012 (see Gootman 2016), are best thought of as CNE or espionage. Equally, it would be useful to think of less serious 'cyberthreats' such as crime and hacktivism as exactly that, crime, (h)acktivism, nuisance – and something that should be dealt with by law enforcement agencies where necessary.

Third, instead of 'cyber-security',[18] we should return to the terms originally developed to characterise the different challenges that fall under the moniker of Computer Network Defence (CND). Each of these has a slightly different meaning and focus, for example; Information Security refers to protecting against unauthorised *use* of data; Network Security to preventing unauthorised *access* to data; and Computer Security involves protecting against *damage* to hardware and software. This also might mean the creation of a new term 'information security hygiene' which refers to human engagement with computers, networks and information, and recognises the importance of the human-machine interface. Lumping all of these under 'cybersecurity' might help draw attention, but at the same time obfuscates the specific requirements of each component. Likewise, it is important to recognise that the term 'cyberdefence' can sometimes be used to refer to active measures to gain access and compromise systems before an adversary has carried out an operation, making it very similar to a CNA.

Finally, it would make sense to treat the terms 'cyberwar', 'cyberwarfare' and 'cyberweapons' with great care, as this is another set of concepts that are often used to mean very different things. Notwithstanding the fact that it currently seems very unlikely that we will experience warfare that only utilises digital 'weapons', takes place solely in the digital realm, and involves hackers rather than soldiers (Lewis 2011), the term 'cyberwar' is often used to refer to ongoing activities that really shouldn't be classified as warfare. Modern warfare will almost certainly *involve* CNOs and IW, but this does not mean that it qualifies as a 'cyberwar' but simply, as war. We are most likely to see CNO and IW used in conjunction with other forms of military force. Indeed, the U.S. 'Joint Concept for Access and Maneuver in the Global Commons' and recent Chinese military doctrine makes this explicit. Moreover, penetration testing, espionage, and 'buzzing'[19] defences are established (if not necessarily desired) parts of international relations and fall well below what one might consider an act of war. In terms of 'cyberweapons' there is a marked difference between hackers that breach systems, steal information or delete files, and those that build and deploy a specific piece of coding for a specific purpose (Rid and McBurney 2012). The Oxford English Dictionary describes a weapon as 'A thing designed or used for inflicting bodily harm or physical damage', which clearly only applies to a handful of Computer Network Operations.

While it is difficult to think of a circumstance where 'cyber' is the best descriptor for the purposes of the academic and policy debate, it may still have a role to play at a very general level in public fora and in raising awareness, but this linguistic parsimony comes at an analytical cost. As such, we should also be careful about the notion of currently living through a 'cyber' age – again the semantics here are important. We are certainly living through a period of significant flux in the global information environment, but this could easily be traced back to the invention of the telegraph in the mid-1900s, or to the first modern digital computers in the second half of the twentieth century.

Conclusion: building security through language

The confusion and misunderstanding that surrounds the use of the word 'cyber' in security, strategic and military studies and in policymaking is in danger of making the concept hollow and perhaps even meaningless when we talk about the challenges posed to computer systems and networks. At best, it is prohibiting a more fruitful academic and policy debate on the nature, extent and implications of the latest information age; at worst it is preventing us from getting to grips with serious and pressing threats to our way of life. Too often the same phrase is used to mean entirely different things, and more often still the 'cyber' moniker appears to be used (irresponsibly in some cases) to add increased seriousness or importance with little or no thought as to how this is grounded in our broader understanding of the concept. The result is that much of the 'cyber debate' – particularly in the social sciences – has become hyped and distorted, with worst-case predictions based on relatively little evidence or research abounding. The pace of technological change (for example, the advent of artificial intelligence, machine autonomy and their relationship with information technology) makes this task even harder. At least part of the reason for this is that the 'cyber revolution' is still in the words of Lucas Kello 'incipient' (2013, 39) and the legitimate field of enquiry is still being established, but there seems little point proliferating this literature until some basic principles and common language can be established or agreed. The same also applies to those within government and international institutions wrestling with how to respond to the latest apparently all-encompassing security buzzword.

As a result, there is a strong case for retiring the term 'cyber' from both academic and policy discourse and debates, and letting it return to the world of science fiction from where it came (this may even happen organically in the long-run[20]). In the first instance this will involve revisiting the language originally developed by computer science, such as Computer Network Operations, Computer Network Attack, Computer Network Exploitation, Computer Network Defence, Information Security and Computer Security, etc. It is difficult to think of many uses of the 'cyber' prefix where it might not easily be replaced by the word's 'information', 'computer', 'digital' or 'electronic' (information security; computer attack; digital weapons; electronic warfare, for example). Secondly, when addressing the problem, it will require scholars and policymakers to differentiate between: (i) the challenges posed by the digital real-time context that shapes the contemporary security environment, and what and how decisions are made; a new 'domain' of operations, and the various tools and capabilities that might be used against computer systems and networks; (ii) between activities that primarily target information and the information space, and those that target information systems directly; (iii) between the means and methods by which an activity or operation is carried out, and the intended target, intention or desired effect being sought; (iv) between the intentions and capabilities of different actors; and (v) between *who* should be responsible for responding or securing against the threat – individuals, companies and organisations, law enforcement agencies or national governments. Finally, we might need to accept in the short and medium term that grand frameworks, definitions and theories intended to conceptualise and understand the multifaceted impact of the latest information age might not be the most productive way forward. A better approach could be to encourage diversity and issue-specific frameworks of analysis, but only if these are made clear and explicit as part of

the argument being made. No one approach should necessarily predominate; instead we might be better served increasing the stockpile of detailed studies and data from which to draw upon.

It is an unusual thing to call for the retirement of a word, but the complicated genesis, myriad conceptualisations and applications of 'cyber', and the way that it has hampered rather than helped in shaping academic debates and formulating policy, means that it is only serving to complicate rather than address the challenges of a new digital context. In a sense, what appears to have happened is that social science has hijacked a concept that emerged from the hard sciences, especially computing and IT, and discarded the terminology and vocabulary developed and used by those who understood these technological dynamics best. This may have had some use in the 1980s and 1990s in drawing attention towards a new phenomenon, but that now digital networks are ubiquitous, apart from in the most general sense, the term has now essentially become banal. Social scientists undoubtedly have a pivotal role to play in understanding, conceptualising and managing the impact of new technology on our world, but this must be a multi-disciplinary conversation across society given the plethora of stakeholders involved, where the best insights and expertise from across the board can be utilised. It must also be a conversation where we know what people are talking about, and where we are clear what questions, issues and topics are on the table and in what fora. An academic and policy world characterised by far more linguistic clarity, precision and acceptance is the only way to properly begin to understand, conceptualise and mitigate the most pressing security challenges of the current information age.

Notes

1. US Secretary of Defense Leon Panetta famously warned of a 'cyber Pearl Harbor'.
2. A good example of this, as David Sanger explains, is that 'Acts that the United States calls "cyber network exploitations" when conducted by American forces are often called "cyberattacks" when American citizens are the target' (2018, xiv).
3. To a lesser extent this is what has happened with the word 'security' since Barry Buzan, Ole Waever, and Jaap de Wilde published *Security: A New Framework for Analysis* in 1997, and with the concept of 'hybrid warfare' (which itself has become commingled with 'cyber'). Similar problems exist with words such as 'culture'.
4. Cyberpunk is described by the online urban dictionary as 'a subgenre of sci-fi in which there is a strong sense of helplessness, misery, dystopic ideals and loss of morality and/or humanity. Corporations control the lives of their workers and reside in microcosms dictated by the status quo'. http://www.urbandictionary.com/define.php?term=cyberpunk.
5. The current epoch can probably be thought of as the second information age. The first refers to the development of the telegraph in the mid-nineteenth century. See Brock (2003).
6. According to Kaplan, cyber was the name advocated by Michael Vatis, a Justice Department lawyer on the working group who had just read *Neuromancer*.
7. The Tallinn Manual is not a *globally* accepted agreement on definitions.
8. See: https://en.oxforddictionaries.com/definition/cyber.
9. Bugs are errors in coding and *not* the result of deliberate interference or attack (although they are often a key way into systems for hackers).
10. Notwithstanding the WannaCry attack believed to have been designed by North Korea to gain foreign currency.
11. For example, the solar sunrise attack against the US defence networks in 1998 – while not highly sophisticated – was carried out by a pair of 16-year-old boys from San Francisco.

Then Deputy Secretary of Defense, John Hamre warned that this could be 'the first shots of a genuine cyber war' (quoted in Kaplan 2016, 74).

12. Similar to a nuclear weapon, we can think of some 'cyber weapons' as having a delivery vehicle (a way into a system) and a warhead (the code designed to do something to that system when it has been breached).
13. Moreover, CNOs are usually only deadly if they unleash the power and destructive potential already inherent within a system.
14. There is a parallel with the use of the term 'WMD', especially in relation to the claims made before the 2003 Iraq war.
15. Social Engineering is the use of online deception to trick individuals into disclosing private or personal information (i.e. through email phishing scams) or collecting information from social media such as Facebook, that can then be exploited by criminals or states (See Mouton, Leenen, and Venter 2016; Heary 2009).
16. Although Nye still uses cyber as a one-size-fits-all descriptor in his analysis.
17. The Budapest Convention on Cyber Crime signed in 2001 is an example of a different approach. See http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
18. For a good overview of industry perspectives on this term, see (Kobie 2017).
19. A term used to refer to flying military aircraft close to an adversary's air defences and borders.
20. As William Gibson, author of *Neuromancer* put it, '"Cyberspace" as a term is sort of over. It's over in the way that, after a certain time, people stopped using the suffix "-electro" to make things cool, because everything was electrical. "Electro" was all over the early 20th century, and now it's gone. I think "cyber" is sort of the same way' (quoted in Phillips 2016, 189).

Acknowledgements

The author would like to thank David Blagden, Bleddyn Bowen, James Johnson, Mark Phythian, and Elke Schwarz.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by Economic and Social Research Council [ES/K008838/1].

Notes on contributor

Andrew Futter is an Associate Professor of International Politics at the University of Leicester, U.K. He is the author of five books, the most recent 'Hacking the bomb' was published by Georgetown University Press in 2018. He is a recent Visiting Scholar at the Nobel Peace Institute in Oslo.

References

Ablon, L. 2015. "Social Engineering Explained: The Human Element in Cyberattacks." *RAND Cipher Brief*, October 20. https://www.rand.org/blog/2015/10/social-engineering-explained-the-human-element-in-cyberattacks.html.

Anderson, R. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis, IN: Wiley Publishing.
Andress, J., and S. Winterfeld. 2011. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Waltham, MA: Syngress, Elsevier.
Arquilla, J., and D. Ronfeldt. 1993. "Cyberwar is Coming!" *Comparative Strategy* 12 (2): 141–165.
Bate, L. 2015. "Stop Calling Everything 'Cyber'." *The National Interest*, October 14. http://nationalinterest.org/feature/stop-calling-everything-cyber-14070.
Berkowitz, B., and R. Han. 2009. "Cybersecurity: Who's Watching the Store?" *Issues in Science and Technology* 19 (3). http://issues.org/19-3/berkowitz-2/.
Brock, G. W. 2003. *The Second Information Revolution*. Cambridge, MA: Harvard University Press.
Buzan, B., O. Waever, and J. de Wilde. 1997. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.
Cirenza, P. 2016. "Cyberweapons Aren't Like Nuclear Weapons." *Slate*, March 15. www.slate.com/articles/technology/future_tense/2016/03/cyberweapons_are_not_like_nuclear_weapons.html.
Collins, J., and A. Futter. 2015. *Reassessing the Revolution in Military Affairs: Transformation, Evolution and Lessons Learnt*. London: Palgrave.
Denning, D. 1999. *Information Warfare and Security*. Reading, MA: Addison-Wesly.
Futter, A. 2016. *Cyber Threats and Nuclear Weapons – New Questions for Command and Control, Security and Strategy*. London: RUSI.
Futter, A. 2018. *Hacking the Bomb: Cyber Threats and Nuclear Weapons*. Washington, DC: Georgetown University Press.
Giacomello, G. 2010. "Bangs for the Buck: A Cost-benefit Analysis of Cyberterrorism." *Studies in Conflict and Terrorism* 27 (5): 387–408.
Gibson, W. 1984. *Neuromancer*. New York: ACE.
Giles, K., and W. Hagestad II. 2013. "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English." In *Proceedings of the 5th International Conference on Cyber Conflict*, edited by K. Potins, J. Stinissen, and M. Maybaum. Tallinn: NATO CCD COE Publications.
Gootman, S. 2016. "OPM Hack: The Most Dangerous Threat to the Federal Government Today." *Journal of Applied Security Research* 11 (4): 517–525.
Graham, C. 2017. "NHS Cyber Attack: Everything You Need to Know About the 'Biggest Ransomware' Offensive in History." *The Telegraph*, May 20.
Heary, J. 2009. "Top 5 Social Engineering Exploit Techniques". *PCWorld*, November 14. https://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html.
Kaplan, F. 2016. *Dark Territory: The Secret History of Cyber War*. London: Simon & Schuster.
Kello, L. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7–40.
Kenney, M. 2015. "Cyber-terrorism in a Post-Stuxnet World." *Orbis* 59 (1): 111–128.
Kobie, N. 2017. "Is it Time to Drop 'Cyber' in Security?" *ITPro*, May 31. http://www.itpro.co.uk/security/28733/is-it-time-to-drop-cyber-in-security.
Kramer, F. 2009. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*, edited by F. Kramer, S. Starr, and L. Wentz, 3–23. Dulle, VA: Potomac Books Inc.
Kuehl, D. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, edited by F. Kramer, S. Starr, and L. Wentz, 24–42. Dulles, VA: Potomac Books Inc.
Lafrance, A. 2016. "Trump's Incoherent Ideas About 'the Cyber'." *The Atlantic*, September 27. https://www.theatlantic.com/technology/archive/2016/09/trumps-incoherent-ideas-about-the-cyber/501839/.
Lee, R. M., and T. Rid. 2014. "OMG Cyber: Thirteen Reasons Why Hype Makes for Bad Policy." *The RUSI Journal* 159 (5): 4–12.
Lewis, J. 2011. "Cyber Attacks, Real or Imagined, and Cyber War." *Center for Strategic and International Studies*, July 11. https://www.csis.org/analysis/cyber-attacks-real-or-imagined-and-cyber-war.
Libicki, M. 2007. *Conquest in Cyberspace: National Security and Information Warfare*. New York: Cambridge University Press.
Lindsay, J. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404.

McConnel, M. 2009. "Cyberwar is the New Atomic Age." *New Perspectives Quarterly* 26: 72–77.
Meyer, P. 2011. "Cyber-security Through Arms Control: An Approach to International Cooperation." *The RUSI Journal* 156 (2): 22–27.
Mouton, F., L. Leenen, and H. S. Venter. 2016. "Social Engineering Attack Examples, Templates and Scenarios." *Computers & Security* 59: 186–209.
Newitz, A. 2013. "The Bizarre Evolution of the Word 'Cyber'." *io9*, September 13. https://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487.
Nye, J. 2016/2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44–71.
Owens, W., K. Dam, and H. Lin, eds. 2009. *Technology, Policy, Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*. Washington, DC: National Academies Press/National Research Council. http://www3.nd.edu/~cpence/eewt/Owens2009.pdf.
Panetta, L. 2012. "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security." *New York City*, October 11. http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.
Phillips, P. 2016. *Conversations with William Gibson*. Jackson: University of Mississippi Press.
Rattray, G. 2001. *Strategic Warfare in Cyberspace*. Cambridge, MA: The MIT Press.
Rid, T., and P. McBurney. 2012. "Cyber-weapons." *The RUSI Journal* 157 (1): 6–13.
Sanger, D. 2018. *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. New York: Crown Publishers.
Schmitt, M., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
Singel, R. 2010. "Check the Hype – There's No Such Thing as Cyber." *Wired*, March 26. https://www.wired.com/2010/03/cyber-hype/.
Tabansky, L. 2011. "Basic Concepts in Cyber Warfare." *Military and Strategic Studies* 3 (1): 75–92.
Tadeo, M. 2014. "Israel Army Twitter Account Hacker Issuing 'Nuclear Leak' warning." *The Independent*, July 4. https://www.independent.co.uk/news/world/middle-east/israel-army-twitter-account-hacked-issuing-nuclear-leak-warning-9583846.html.
United States Department of Defense, Defense Science Board. 2013. "Task Force Report: Resilient Military Systems and the Advanced Cyber Threat." January. http://www.acq.osd.mil/dsb/reports/ResilientMilitarySystems.CyberThreat.pdf.
Valeriano, B., and R. C. Maness. 2014. "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11." *Journal of Peace Research* 51 (3): 347–360.
Weimann, G. 2005. "Cyberterrorism: The Sum of all Fears?" *Studies in Conflict & Terrorism* 28 (2): 129–149.
Wiener, N. 1948. *Cybernetics or Control and Communication in the Animal and the Machine*. Cambridge, MA: The MIT Press.
Wolff, J. 2016. "Cyber is Not a Noun." *Slate*, September 9. http://www.slate.com/articles/technology/future_tense/2016/09/cyber_is_not_a_noun.html.
Zetter, K. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.