Defining cyberwar: towards a definitional framework

Cameran Ashraf
School of Public Policy, Central European University, Budapest, Hungary

ABSTRACT
For nearly thirty years scholars have offered changing definitions of cyberwar. The continued ambiguity demonstrates that efforts at establishing definitional clarity have not been successful. As a result, there are many different and contradictory definitions, ranging from cyberwar’s non-existence to cyberwar as an imminent threat. Ongoing definitional ambiguity makes interdisciplinary research and policy communications challenging in this diverse field. Instead of offering a new definition, this paper proposes that cyberwar can be understood through a fluid framework anchored in three themes and five variables identified in a broad interdisciplinary survey of literature. This framework’s applicability is demonstrated by constructing an example definition of cyberwar utilising these themes and variables.

KEYWORDS
Cyberwar; geopolitics; internet; cyber conflict; cybersecurity

Introduction
Despite emerging into public consciousness in the 1980s, no generally accepted definition of cyberwar exists. There are many different and often contradictory definitions, ranging from cyberwar’s non-existence to cyberwar as an existential threat. A clear definition for cyberwar is vital for academic scholarship, security planning, and public policy. Definitional ambiguity makes coherent discussions of cyberwar challenging, limiting theoretical insights, and frustrating efforts at policy development. Indeed, Hughes and Colarik discovered that out of 159 cyberwar articles, 103 (65%) failed to offer an explicit definition of cyberwar.

Awareness of this definitional ambiguity is vital for non-experts in the field for reaching definitional consensus and clarity in research and policy work. To that end, the purpose of this paper is to offer officials, analysts, scholars, and others without expertise in the field an overview of cyberwar’s definitional ambiguity, identify themes in the literature, offer a framework for defining cyberwar, and demonstrate how that framework can be used. While the field is evolving and growing, it is hoped that this paper can provide a conceptual grounding in the ongoing definitional debate over cyberwar.

In examining this interdisciplinary body of literature, three themes were identified: alarmist, skeptic, and realist. Broadly speaking, alarmists see cyberwar as an imminent threat, skeptics believe cyberwar is a contested idea and is not “war”, and realists...
believe that cyberwar should be understood through existing law and norms. These three themes are not mutually exclusive and weave their way through cyberwar scholarship. A single project may contain all three themes in equal measure, be more alarmist than skeptical, or any other configuration. For example, Sanger is alarmist in framing cyberwar as an imminent threat and realist in recognising the role of the state in working with international norms.5

Much of the debate on defining cyberwar focuses on the applicability of existing international law and state practice to cyberspace.6 This perspective believes that attacks in cyberspace can constitute a use of force, allowing a state to act in self-defense.7 These attacks fall under the legal concept of *jus ad bellum*, how a state justifies self-defence. In following this logic, once cyberwar has begun, then cyberattacks fall under *jus in bello*, or the rules governing the process of warfare. How *jus ad bellum* and *jus in bello* apply to cyberwar is constrained within the existing United Nations charter (Articles 2 (4), 39, 41, 51), relevant international legal regimes, and norms of state behaviour.8

However, existing legal frameworks are only partially relevant to actions which do not fall under *jus ad bellum* and *jus in bello*. These actions can be governed by different sets of laws, such as: a) international agreements on cyberspace; b) location-based agreements through which the means of cyberwar are governed, such as the law of the sea, and those governing outer space, transnational communications, and aviation; and, c) international law of counter-measures, which regulate how states respond to violations which do not justify the use of force.

Applying legal regimes, territorial law, and jurisdiction to cyberwar situates it within the legal-territorial framework of the international system of states.9 However, a significant number of territorially ambiguous actions occur outside this framework. These attacks occur in a legal frontier and from a “liberal-utopian” position where cyberwar operates openly across international boundaries.10 The paradox of realist structure and liberal-utopian action is central to the efforts of states to apply a legal-territorial framework to cyberwar. These actions operate across a “spatiality of power” not confined to the limitations of geographical territory.11

### Attempts to define cyberwar

The definitional ambiguity of cyberwar has not deterred academia, military, or governments in attempting a definition. Early definitions and popular media, such as the influential 1983 movie WarGames, and the seminal and provocatively titled 1993 paper *Cyberwar is Coming!* by Arquilla and Ronfeldt,12 established a class of “alarmist” definitions which argued that cyberwar was an imminent threat. The United States and its allies were framed as under threat, necessitating a strong defence and view of cyberspace as a domain where the United States could achieve dominance.13

Alarmist definitions are a recurrent theme in cyberwar thought and policy.14 One of the most influential recent thinkers, former White House counter-terrorism advisor Richard Clarke, argued in his 2010 bestselling book *Cyber War: The Next Threat to National Security and What to Do About It* that cyberwar was “actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption”.15 Clarke’s definition proved to be highly influential in cyberwar
research, and is the most highly cited (in Google Scholar) work on cyberwar, followed by 1990s alarmist work by Arquilla and Ronfeldt.\textsuperscript{16}

Mehan\textsuperscript{17} extends the alarmist model into different classes of cyberwar. Class I cyberwar deals with personal informational security; Class II emphasises espionage; Class III includes (distributed denial of service) DDoS and other disruptive actions; and Class IV incorporates classes I-III in addition to cyber operations in support of military offensive actions. Mehan\textsuperscript{18} does not specify the nature of the actions or the actors involved, leaving cyberwar open to individual hackers, collectives, social movements, terrorists, corporations, and states.

Strategic doctrines have shifted from skepticism about cyberwar to including cyber as a key component of national defense. Alarmist thinking has also shifted from the perspectives offered by Arquilla and Ronfeldt\textsuperscript{19} and Clarke\textsuperscript{20} to more nuanced positions which perceive vulnerabilities not just in the United States, but for global leadership on setting cyberwar norms. This has manifested in nuanced alarmist perspectives from Sanger, Healey, Nye, and others.\textsuperscript{21} These scholars balance emphasis on imminent threats and the need for urgent cybersecurity reforms with an embrace of multipolarity.\textsuperscript{22}

These definitions assert that cyberwar is an urgent threat while maintaining broad definitions of what constitutes cyberwar. For instance, Healey argues that states should focus less on determining attribution for attacks and instead on who should bear responsibility for attacks, stating that “Who is to blame?” can be more important than ‘who did it?’\textsuperscript{23} Alarmists are supported by military and defence policies which warn against an imminent “digital Pearl Harbor”\textsuperscript{24} with statements like “A cyber attack could stop our society in its tracks”\textsuperscript{25} by General Martin E. Dempsey, former-Chairman of the Joint Chiefs of Staff. Alarmism is used in popular rhetoric to support aggressive budgeting in the United States of over $17.4 billion in pursuit of strategic advantage and “defending forward” in cyberspace.\textsuperscript{26} These definitions see cyberwar as everything to anybody at any time and a world in which the West is under imminent threat.\textsuperscript{27}

Another theme used by scholars argues that cyberwar is blown out of proportion and resembles Cold War fearmongering.\textsuperscript{28} In this skeptical theme, “cyberwar” is actually espionage or sabotage with few events, if any, able to be classified as “war” – in fact, cyberwar itself may not even exist.\textsuperscript{29} More theoretical approaches argue that cyberwar is a concept rather than a fact, with Joque stating “it will be fruitful to understand cyberwar as a war against systems: computer systems, state systems, systems of organization, and even systems of meaning”.\textsuperscript{30} Lindsay likewise emphasises that “cyberattack is a form of cheating”\textsuperscript{31} in a cyberspace which is an “assemblage of overlapping regulatory mechanisms and negotiated contracts implemented by both people and machines”.\textsuperscript{32}

To some skeptical scholars, cyberwar has been glorified to benefit defence budgets and a cyber-industrial complex.\textsuperscript{33} Some skeptics, like Rid and others\textsuperscript{34} prefer definitions of cyberwar grounded in state-centric understandings of war. Valeriano and Maness\textsuperscript{35} argue that the actual threat of cyberwar fails to live up to the myth of existential threat, and that “Cyberwarfare poses a threat only if it is grossly overused or mismanaged, or if it diverts resources toward a mythical fear and away from real threats”. For Liff\textsuperscript{36} the realities of cyberwar limit its effectiveness at change into something which emphasises pre-existing political power.

Many of these approaches emphasise nineteenth century theorists, such as Clausewitz. Rid sees Clausewitz as a foundation for defining what cyberwar must be: violent by using
force; instrumental in seeking to force an enemy to change; and with political aims. For many cyberwar skeptics, there has yet to be any action in cyberspace which could satisfy Clausewitz’s definition of war. The actions which have occurred and will likely occur are espionage, sabotage, or subterfuge but nothing resembling “war.”

Rid’s approach is ends-based and focuses on war when it emerges rather than what contributes to causing war. From this perspective, the StuxNet attacks against Iran’s nuclear programme would not be cyberwar because they lacked the critical element of lethal force. Further, the plausible deniability associated with cyberattacks makes determining the political, or instrumental, reasoning behind these acts difficult, reinforcing the Clausewitzian position.

The realist theme grounds cyberwar within existing legal regimes and structures. Rather than arguing cyberwar is imminent or does not exist, these scholars believe it can be understood using existing international law and norms of state behaviour. This perspective includes publications from NATO which determine how international law applies to cyberwarfare. Manjikian argues that this theme is a realist interpretation of cyberspace within existing power structures and geographies which can be adapted to law with minor modifications. Whetam addresses skeptics directly by demonstrating that “war” as an easily definable event is a modern invention. He shows that medieval warfare was practiced on a scale ranging from conventional large-scale pitched battles to ongoing small-scale raids, and that the entirety of this spectrum was considered war:

Real war takes place on a spectrum, framed by the unattainable concept of absolute war at one end and the absence of war at the other. That spectrum should, rightly, include cyber-attacks that do no obvious physical harm.

Beyond this, Hathaway, Clarke, and the Tallinn Manual situate cyberwar as occurring between states grounded within the United Nations charter and international legal agreements and practice. Non-state actors are treated as aberrations, regardless of whether these actors are assisting states in upholding or violating international law. Crowdsourced attacks, such as those which occurred against Iran in 2009, against various Arab states in 2011, or against financial firms which declined to process payments for WikiLeaks, are examples of when this approach encounters problems. Nonetheless, Eun and Aßmann believe that it is not cyberwar that must conform to our definitions of war, but rather that war must conform to new realities of conflict.

From a norms perspective, Clarke argues that states which sanction cyberattacks would be disconnected from the Internet until the attacks stop, an idea with precedence in international finance. Conceptually this is echoed in Healey, whose work is both alarmist and realist, and argues that technical focus on attribution detracts from the ability to address cyberattacks required by the policy world. He states:

To rein in attacks raging across the Internet, the international security community must focus on the needs of policy makers, which is best served by looking to the responsibility of nations. Too much time has been wasted obsessing over which particular villain pressed the ENTER key.

According to some of these definitions, the state is the only geographical unit of analysis because of its unmatched financial and technical resources. Indeed, Lindsay and Betz argue that only states have the resources to conduct cyberwar or develop
complex cyberweapons such as StuxNet. They are skeptical of the resources of non-state actors to engage in complex attacks and scale to rise to the level of “war”. However, these definitions ignore that states outsource cyberwar to hackers, quasi-government organisations, private citizens, terrorist organisations, and criminal groups. To that end, the realist theme does not confine the actors to states, but also includes non-state actors. Here Lucas states that “international law is inherently state-centric, while the cyberdomain is without discernible or meaningful state boundaries or jurisdictions.”

**Three themes: a framework for defining cyberwar**

Each theme in the literature emphasises certain actions, actors, effects, geography, and targets of cyberwar. A framework for defining cyberwar must include these variables while incorporating the broad historical themes in the literature. First, however, the following historical themes have been identified:

**Alarmist:** Cyberwar is an immediate present danger to the United States and its allies.

**Skeptic:** Cyberwar as both concept and reality is contested and ambiguous, and its existence depends on how we define cyberwar.

**Realist:** Some form of conflict in cyberspace exists, and it can be understood through existing international legal structures and state behavior norms.

The table below summarises the three themes of cyberwar literature alongside the five variables of cyberwar definitions (Table 1):

**Key variables**

The key variables of each theme are actions, actors, effects, geography, and targets and are explained below:

**Actions:** Defining cyberwar requires defining which actions are part of cyberwar. There has been much debate on defining cyberattacks and their relationship to violence. For example, during the 1990s, DDoS attacks and defacement were considered hostile acts which could cripple vital communications. During Russia’s 2008 invasion

| Variable | Explanation | Alarmist | Skeptic | Realist |
|----------|-------------|----------|---------|--------|
| Actions  | Nature of hostile actions in cyberspace | Cheap and widespread | Expensive and complicated | Both |
| Actors   | The “legitimate” actors in cyberwar | Anyone/anything; final responsibility is with states | States | Anyone/anything |
| Effects  | Possible effects of cyberwar | Large-scale disruption or destruction, military decapitation | Small-scale, local disruption; ideas and concepts | Legal implications for international state system |
| Geography | Where cyberwar takes place | Cyberspace is separate, but may intersect with physical space | Cyberspace is only proxy for physical space | Cyberspace and physical space are legally and practically indistinguishable |
| Targets  | The targets of cyberwar | Critical state, military, or private infrastructure/information | Critical infrastructure, information, human beings | Military targets, individuals, corporations, states |
of Georgia and 2007 cyberwar with Estonia, these tactics were used to great success in order to create “information dominance”. However, recent research argues that these acts have diminished in importance as robust defences are common. Instead, these acts are now acts of disobedience or mild disruption. The changing nature of defining actions is a function of cost and complication of attacks. Stuxnet, for example, was exceptionally complex and could only have been developed with the resources of a nation-state. In this variable, actions are either cheap and widespread, as with DDoS, or expensive and complicated, as with Stuxnet, reflecting the split between alarmist and skeptic.

**Actors:** Actors are the legitimate entities that can both engage in and be responsible for cyberwar. Defining actors represents a way in which legitimacy is conferred, allowing certain responses in line with how the actors are classified. For example, the 1999 attacks against NATO computers had their origin in Chinese-sponsored groups portrayed as “patriotic citizens”. Rather than attempting to engage with the individual citizens or their actions, NATO chose to recognise China as the entity which had ultimate control over the attacks – legitimising the state as the actor in cyberwar. Generally, cyberwar literature focuses states, non-state actors, or everyone as legitimate actors in cyberwar.

**Effects:** Actions and actors seek outcomes and effects, and each of the themes defines cyberwar by the effects of cyberattacks. Clarke argues that the effects of cyberwar are large-scale destruction with societal collapse or severe disruption. On the other hand, Rid argues that the effects are small-scale: localised intelligence-gathering, or mild disruption in information flows within closed organisational structures. Sanger takes a broader view, eschewing scalar limitations and emphasising that future cyberwars will be long-term and low-intensity with a mix of both large and small-scale actions.

**Geography:** How actors relate to cyberspace conditions how cyberwar is perceived. The skeptical theme generally sees cyberspace as a separate and proxy-domain which is self-contained with little spillover into the “offline” world. For these scholars it follows that cyberwar’s effects would be small-scale. Conversely, the alarmist theme sees cyberspace as a warfighting domain conceived of in terms of national territory, making incursion an act of cyberwar. Each theme constructs a different vision of cyberspace which reflects the actions, actors, and effects of cyberwar.

**Targets:** Ultimately, actions, actors, effects, and geography are also structured around the types of targets for cyberattacks. For example, alarmist definitions view critical infrastructure, such as electrical power plants, as prime targets for cyberwar. On the other hand, skeptics argue that these targets are already well-protected, meaning that smaller and less consequential or purely conceptual targets remain. Targets serve to reinforce and ground the geographical visions of each theme.

Each of these five core variables of cyberwar will be examined through the lenses of the three themes (alarmist, skeptic, and realist) below:

**Alarmist**

The alarmist theme argues that cyberwar is an imminent threat. Within the literature these scholars advocate for immediate action, leveraging Cold War or “clash of civilizations” geopolitical frameworks alongside focus on opponents such as China and Russia.
These scholars share a Hobbesian worldview of cyberspace as a digital “all against all”, in contrast with others who see collaborative potential in cyberspace.72

*Actions:* Alarmism believes that the technical knowledge and cyberattacks are cheap, easy to duplicate, and widespread.73 This framing situates the United States and its allies under immediate threat of cyberwar from hackers who could easily challenge the state. Defences, however, are costly and require concerted national effort to secure critical infrastructure.74 The United States and its allies are believed to be highly vulnerable to attacks of varying destructive capability, with an emphasis on destructive rather than disruptive actions.

*Actors:* The belief that actions in cyberspace are cheap and widespread lends itself to the belief that actors are also widespread. These include individual hackers, terrorists, states, social movements, and corporations. Compromised computers or Internet of Things devices can also be actors, programmed to automate attacks or discover exploits.75 The multiplicity of actors does not imply that all actors are equal, or legitimate. The emphasis is on states as hostile actors who employ non-state actors for plausible deniability. For alarmists, ultimate responsibility resides with the state for financing attacks, allowing use of their national cyberspace, or refusing to cooperate with investigations into attack responsibility.76

*Effects:* Alarmist scholars emphasise the destructive aspects of cyberwar.77 Technical and infrastructural destruction will have unforeseen consequences for society, necessitating an emphasis on defending forward or responding to cyberwar with physical force.78 Alarmists believe that vulnerability of technical systems could cause power outages, water-processing malfunctions, air-traffic control shutdowns, and railroad collisions, among other disasters.79 In addition, alarmist scholars believe that cyberwar can be used to decapitate military command and control, resulting in battlefield chaos.80

*Geography:* For alarmists, the geography of cyberwar is bifurcated between cyberspace and physical space, both existing within national territory. While cyberwar can spillover into physical space, it remains a separate domain in terms of defensive and offensive actions, articulated here by the United States Department of Defense:

A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.81

This domain requires human-made technologies to enter and exists apart from other domains.82 However, it has consequences for other domains (land, air, sea, space) and requires unique rules of engagement, codified in the world’s militaries since the 1980s.83

*Targets:* The targets of cyberwar are critical national infrastructure. This includes physical infrastructure, such as electricity and transportation, financial systems, information and media, intellectual property, consumer data, and communications.84 Because infrastructure is diverse and varies in cybersecurity preparedness, it is both vulnerable and vital - an attractive target during cyberwar. There is a firm sense of the state as spatial container of cybersecurity and any violation of that space represents a physical threat to the state itself.85

*Summary:* The alarmist theme articulates defined national boundaries which are a container for vulnerability and cybersecurity. The domain of cyberspace is separate from physical and political geography, but conflict in this domain has serious effects offline. National territory exists online and offline and is under threat from external
attackers armed with cheap and widely-available cyberattacks. At stake is critical infrastructure with the potential for destruction, resulting in serious disruption in the functioning of society.

Alarmists use a range of historical vulnerabilities in cybersecurity to support their perspective. One of the prominent examples is operation Moonlight Maze. This operation targeted the U.S. Air Force, NASA, the Departments of Energy and Defense, and major universities and research laboratories across the country. Highly sensitive data was exfiltrated, including maps of military installations, and military hardware schematics. Other similar attacks used by alarmists to demonstrate vulnerability of the state and the widespread nature of cyberwar include the Gh0stNet cyberespionage ring and Titan Rain.

Skeptic

The alarmist position has been influential since cyberspace was recognised as a threat domain after the Morris Worm attack in 1988. These entrenched attitudes have been challenged by skeptics who contest the existence, scope, and severity of alarmist definitions. Skeptics argue for critical engagement with the idea of cyberwar, deconstructing the word and its actions to understand the concept. This engagement ranges from denial that cyberwar exists to reconceptualising digital violence. These scholars share skepticism towards the alarmist claims and a desire to shift the debate from “cyberwar is inevitable” towards critically interrogating cyberwar itself.

**Actions:** The skeptic theme argues that actions of cyberwar are not widespread and inexpensive, but costly and expensive. They cite the significant investment in a technology like StuxNet, the availability of resources for attribution, or the extensive insider knowledge needed to hack into critical infrastructure as examples of high barriers to entry. These barriers prohibit actors other than states from engaging in serious cyberattacks. Even then, these are not acts of war, but disruptive acts of sabotage, espionage, and subversion.

**Actors:** Due to expense and complexity, cyberwar is restricted to states. States may outsource actions to non-state actors, but only states have the financial resources to support projects like StuxNet. Shorter term events, such as activist group Anonymous hacking websites of U.S. financial firms, are limited due to lack of state funding. If other actors, such as motivated citizens, universities, private corporations, and other elements of state collective cyberpower can have any impact, it is only because of explicit or implicit state support.

**Effects:** Skeptic scholars contest claims that cyberwar is an existential threat. Concerns over lax security and vulnerabilities in national infrastructure are tempered by claims that exploiting those vulnerabilities requires expert knowledge. Critical infrastructure, they argue, has security measures for malfunctions or catastrophic failures and is well-prepared to address cyberwar vulnerabilities. The effects, if any, of cyberwar are limited and localised rather than significant and widely destructive, or geographically contextualised as a regional issue between rivals. Instead, cyberwar asks us to reconsider how we think about war and violence.

**Geography:** There is nothing unique or special about cyberspace – it is simply another political structure through which states engage in subversion, sabotage, and espionage.
with plausible deniability, and a lack of attribution. Cyberspace as a separate warfighting domain reflects the interests of lobbyists and elites rather than any inherent attribute of cyberspace.

**Targets:** In-line with their belief that cyberwar is of limited scope, its targets are also limited. StuxNet, although its ultimate target was nuclear centrifuges, had as an intermediary target a human being who could transport the malware into the Natanz network, or who could be targeted via phishing. Other forms of cyberwar (espionage, sabotage, or disruption) require human failings or specific expertise to succeed, and only then can any secondary effects be manifested. Thus, the skeptical theme articulates targets both in terms of humans as well as critical infrastructure and information.

**Summary:** Skeptical scholars question the saliency of claims that cyberwar is an existential threat. Cyberwar exists on a spectrum or is discrete components – espionage, sabotage, or subversion – and causes disruption rather than destruction. These actions are expensive and require specialised knowledge, limiting them to being supported by states. Because of high barriers to entry and precautions already in place in most critical infrastructure, the effects of cyberwar are limited and local. Cyberspace is an extension of the physical domain and political actions which occur in it. The existence of a separate warfighting domain reflects lobbying efforts by cyber-security firms, military, and policy elites.

Skeptical claims centre on research which demonstrates that the cost of attack, such as StuxNet, could only be borne by a state, or the lack of explicit physical violence and harm from cyberattacks. For instance, Rid claims that Moonlight Maze does not represent a case of cyberwar, but is an example of cyber-espionage. Likewise, the 2007–08 DDoS attacks on Georgia and Estonia by Russia were a nuisance not a threat.

The skeptical position has found resonance in popular media and in critical studies scholarship. The lack of any significant cyberwar, despite hype by alarmists, has contributed to skepticism that cyberwar will occur. National security experts continue to argue for a more alarmist-based position, but now temper warnings with skeptical considerations, emphasising the idea of cyberwar as disruptive, not destructive.

**Realist**

The third theme involves scholars and practitioners who emphasise that cyberwar exists within a modified realist framework. These scholars do not dispute that cyberwar is a contentious topic. Rather, they see cyberwar as a conceptual, practical, political, and legal frontier which can be understood in historical or current state behaviour and international law.

**Actions:** For the realist theme, there is little distinction between expensive, or complicated actions and cheap or widely available ones. Actions are precipitating an understanding of the legal contexts in which they should be situated – only then can they be understood. To an extent, this is an argument which echoes skeptical contentions about the nature of cyberwar, but realists situate the debate around definitional ambiguity.

**Actors:** The realist conception of actions lends itself to a broad conception of cyberwar – individuals, non-state actors, states, social movements, corporations, and others can all
freely engage in cyberwar. This emphasises individual actors, groups, and networks in cyberspace rather than restricting or limiting actors. Thus, a highly motivated individual could engage in cyberwar, as well as a state, or social movement. What matters is how actors relate within the context of the international system and how norms and law include those actors.

Effects: The realist position is concerned about the implications of cyberwar for international law and politics. These may be disruption, destruction, subversion, espionage, or sabotage, but the impact will be on future interactions between individuals, groups, political and financial structures, intellectual property, and trade regimes. The effects of actions in cyberspace are on the broader systems and the worlds which actions enable. Thus, understanding where a state begins in cyberspace, what constitutes a hostile act, or how to interpret the StuxNet attack in international law, are the effects of cyberwar.

Geography: The realist position sees cyberspace as a domain where unique actions take place, but those actions are grounded in pre-existing physical, political, and legal geographies. It is indistinguishable from the existing international system and must be seen, evaluated, and acted upon as an ordinary feature of that world. This perspective would contest the U.S. Department of Defense’s vision of cyberspace as a separate warfighting domain or the skeptical position that cyberspace is a proxy or metaphor for physical space.

Targets: The focus of cyberattacks are any assets which exist within sovereign territories and legal jurisdictions. This includes civilians, corporations, military networks, and government computers, anything situated within existing international legal structure. What is relevant is the legal and conceptual geography of those targets.

Summary: The theme of realism is concerned with the implications of cyberwar on international law and practice. The precedents established by actions can have unforeseen consequences for international stability and careful analysis must be undertaken to properly understand them. Realism is not concerned with the cost or complexity of actions, but with the “who, what, and where” of cyberwar. Here, states are relevant because they underpin the international system and their actions have bearing on legal precedent and norms.

The realist position is largely composed of legal scholars and academics who see the debate between alarmists and skeptics as focused on language, rather than on events. Whether or not cyberwar exists is an issue about how cyberwar is defined rather than what is occurring in cyberspace. For example, StuxNet may or may not be an act of cyberwar or sabotage. Rather, it is the development and deployment of software, which destroys centrifuges without attribution or accountability and is a threat to international stability. In this example, realists are interested in interpreting events within international law rather than arguing whether cyberwar exists.

Example: using the framework for a definitional compromise

The framework of five variables and three themes can be used by scholars to develop definitions of cyberwar, or understand how themes relate to each variable. Considering the development of critical cyberwar scholarship, recent research has moved away from strict thematic boundaries, bringing together all three themes to paint a more nuanced
picture of cyberwar. For instance, attack types previously considered to be cyberwar, such as DDoS attacks against Estonia\textsuperscript{131} are now seen by the Council of Europe and many scholars as civil disobedience.\textsuperscript{132} The proposed framework reflects emergent patterns of scholarship and the need to move beyond strict themes and towards a more fluid framework for defining cyberwar.

To demonstrate usage of the framework, this paper provides an example fourth theme: a definitional compromise amongst the three other themes. Given the interplay between alarmist, skeptic, and realist themes across literature, this theme sees cyberwar as actions undertaken by states to alter information, disrupt computer systems, networks, or Internet-connected devices belonging, or deemed critical to, another target state. This theme demonstrates how cyberwar can be defined using the framework by supporting each variable with case studies and selecting variable definitions from each theme.

**Defining the variables**

*Actions:* In line with skeptics, cyberwar actions are expensive and complicated. While cyberattacks range from simple DDoS to the highly complex Stuxnet malware, for an action to be considered part of cyberwar it must be complex enough to require state resources. This distinction matters because greater resources allow for more sophisticated attacks, including expensive zero-day exploits which the RAND Corporation estimates costs nearly $30,000 on average.\textsuperscript{133} This does not preclude simple attacks like DDoS, because state resources can be leveraged to execute large-scale attacks, such as Iran’s Operation Ababil DDoS attacks, which temporarily disrupted the U.S. banking sector.\textsuperscript{134}

Beyond cost, critical state infrastructure has well-established protocols and procedures for dealing with emergency situations, necessitating a greater investment in resources by the attacker to infiltrate target networks.\textsuperscript{135} To disrupt in a serious fashion state infrastructure requires specialised knowledge and access to advanced plans or technical specifications, precluding all but the most well-funded and sophisticated actors.

*Actors:* The legitimate actors are states, who bear responsibility for what occurs within their cyberspace. As Healey argues, “national policy makers often need to know the responsibility for an attack, not the technical attribution, to drive their decisions and responses.”\textsuperscript{136} It is not that non-state actors cannot conduct cyberwar actions, but that they often do so on the behalf of states for plausible deniability.\textsuperscript{137} Noteworthy examples of this include the 2016 Russian “Fancy Bear” hacks of the U.S. Democratic National Committee and the Iranian “Shamoon” hacker group responsible for a significant attack on Saudi Aramco, wiping the hard drives of over 30,000 computers in 2012.\textsuperscript{138} However, final responsibility rests with states.

*Effects:* The effects of cyberwar have included not only the destruction of centrifuges, but also the Syrian Electronic Army hacking the Associated Press’ Twitter account and the resulting $130 billion in losses on the S&P 500 index.\textsuperscript{139} It has included long-term disinformation campaigns by Russia, hacks of Sony emails by North Korean mercenaries, and website defacements by Iranians.\textsuperscript{140} The effects of cyberwar are the accumulation of both large and small-scale attacks between adversaries. As Harknett and Smeets argue, “cyberspace introduces new ways and means of degrading national power by attaining
strategic impact through continuous campaigns comprised of often-covert, less violent cyber operations.”

**Geography:** Cyberspace is a distinct and separate domain with protocol-based limitations which limit state actions. That domain is inclusive and constitutive of political geography, meaning that cyberspace is part of a national territorial sovereignty while reconfiguring that sovereignty online. This is illustrated in the 2018 U.S. Department of Defense Cyber Strategy:

The Department will prioritize securing sensitive DoD information and deterring malicious cyber activities that constitute a use of force against the United States, our allies, or our partners. Should deterrence fail, the Joint Force stands ready to employ the full range of military capabilities in response.

This theme echoes the U.S. position by saying there are limitations to warfighting actions in cyberspace, but responses to those actions are not limited by cyberspace. Cyberspace is both part of national sovereignties and a separate domain.

**Targets:** The targets of cyberwar are elements of national cyberpower. Cyberpower is the sum of critical cyber elements of a state and its society, including private corporations, military networks, talented individuals, universities, security organisations, symbols, and social, or political movements. The concept can be understood offensively and defensively, and adversaries may target smaller elements of cyberpower for the purpose of training or gaining access to complex systems. Thus, it may become necessary for states to intervene in non-critical areas which may impact cyberpower. This is demonstrated in the hack of Sony Pictures by North Korean-affiliated hackers. After the hacks, the U.S. government did not respond, believing it an affair for Sony Pictures. Although Sony Pictures was not “critical infrastructure”, eventually the U.S. worried that non-intervention would set a dangerous precedent for national security. Further, the idea of an authoritarian state limiting domestic freedom of expression made intervention symbolically important, with the secretary of the Department of Homeland Security stating “It was also an attack on our freedom of expression and way of life.” Soon, the U.S. government accused North Korea of responsibility for the hacks.

The table below highlights this example within the paper’s framework (Table 2):

### Addressing definitional shift

Definitional shift contributes to the lack of any single broadly accepted definition of cyberwar, and efforts to define cyberwar must address this shift. This paper has conducted a broad survey of interdisciplinary literature to provide an overview of the debates in scholarship, and identified three themes and five variables to provide a framework for defining cyberwar. The definition in this paper is one example of how the conceptual framework can be configured and reconfigured to create new and relevant definitions of cyberwar. Given cyberwar’s definitional fluidity, new definitions may make interdisciplinary communication and policy difficult. Thus, having a base framework for development, understanding, and evaluating definitions creates a common foundation for discussing cyberwar.
Definitions of cyberwar will undergo changes over time, but a modular framework of realist, alarmist, and skeptic provides a flexible baseline for examining future actions in cyberspace and how they relate to the actors, actions, geography, effects, and targets of any future cyberwar. As new technologies and state/non-state behaviours emerge, the framework provides a broad structure for incorporating, evaluating, and understanding change.

### Conclusion

For nearly thirty years scholars have offered changing definitions of cyberwar, and the continued lack of clarity demonstrates that efforts at establishing a singular definition have not been successful. This paper takes the position that a broadly agreed upon scholarly definition of cyberwar is unlikely to emerge. Demonstrating the breadth of definitional ambiguity, Hughes and Colarik identified 56 explicit and 103 implicit definitions of cyberwar currently in use.

The lack of definitional clarity makes interdisciplinary research and policy work challenging. For example, international legal scholars advising policymakers might examine research in security studies or geopolitics to understand attribution. Each of these three fields could have a different definition of cyberwar, leading to policy outcomes which do not speak to current or future realities. As such, it is vital for scholars and policymakers to have a baseline of definitional clarity from which to work.

To address this issue, rather than offering a new definition, this paper offered a framework for understanding the scholarly definitions of cyberwar, focused on three themes identified in a broad interdisciplinary survey of the literature: alarmist, skeptic, and realist. It subdivided these themes by five identified variables: actors, actions, geography, targets, and effects. Subsequent work can interrogate and engage with each aspect of this

---

**Table 2. Alarmist, skeptic, and realist positions and example theme.**

| Variable       | Explanation                                                                 | Alarmist                                                                 | Skeptic                                                                 | Realist                                                                 | Example                                      |
|----------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------|-------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------|
| Actions        | Nature of hostile actions in cyberspace                                    | Cheap and widespread                                                    | Expensive and complicated                                              | Both                                                                    | Expensive and complicated                   |
| Actors         | The “legitimate” actors in cyberwar                                        | Anyone/anything; final responsibility is with states                    | States                                                                  | Anyone/anything                                                         | States                                       |
| Effects        | Possible effects of cyberwar                                               | Large-scale disruption or destruction, military decapitation             | Small-scale, local disruption; ideas and concepts                      | Legal implications for international state system                      | Accumulation of large and small-scale attacks/disruption |
| Geography      | Where cyberwar takes place                                                 | Cyberspace is separate, but may intersect with physical space          | Cyberspace is only proxy for physical space                            | Cyberspace and physical space are legally and practically indistinguishable | Cyberspace is separate, but intersects and is part of physical space |
| Targets        | The targets of cyberwar                                                    | Critical state, military, or private infrastructure/information          | Critical infrastructure, information, human beings                     | Military targets, individuals, corporations, states                    | All elements of national cyberpower           |

---

C. ASHRAF
matrix, demonstrated by the paper’s definitional compromise theme. This framework provides a baseline for developing, understanding, and evaluating definitions of cyberwar across the literature while creating a foundation for future work in this fluid and dynamic field.

Notes
1. Michael Warner, ‘Cybersecurity: A Pre-History’, *Intelligence and National Security* 27, no. 5 (2012): 781–99.
2. Oona A. Hathaway et al., ‘The Law Of Cyber Attack’, *California Law Review* 2012 (2011): 76.
3. Adam P. Liff, ‘Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War’, *Journal of Strategic Studies* 35, no. 3 (2012): 401–28.
4. Daniel Hughes and Andrew Colarik, ‘The Hierarchy of Cyber War Definitions’, in *PacificAsia Workshop on Intelligence and Security Informatics* (Springer, 2017), 15–33.
5. David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*, Reprint edition (New York: Broadway Books, 2019).
6. Richard W. Aldrich, ‘The International Legal Implications of Information Warfare’ (DTIC Document, 1996); Jason Barkham, ‘Information Warfare and International Law on the Use of Force’, *NYUJ Int’l L. & Pol.* 34 (2001): 57; D. Brown, ‘A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict’, *Harvard International Law Journal* 47, no. 1 (WIN 2006): 179–221; Russell Buchan, ‘Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?’, *Journal of Conflict and Security Law* 17, no. 2 (Summer 2012): 212–27, https://doi.org/10.1093/jcsl/krs014; Dimitrios Delibasis, *The Right to National Self-Defense: In Information Warfare Operations* (Arena Books Limited, 2007); Christopher D. DeLuca, ‘Need for International Laws of War to Include Cyber Attacks Involving State and Non-State Actors, The’, * Pace Int’l L. Rev. Online Companion*, 2013, ii; Louise Doswald-Beck, ‘Some Thoughts on Computer Network Attack and the International Law of Armed Conflict’, *Computer Network Attack and International Law*, 2002; David P. Fidler, ‘Was Stuxnet an Act of War? Decoding a Cyberattack’, *Security & Privacy, IEEE* 9, no. 4 (2011): 56–59; Andrew C. Foltz, ‘Stuxnet, Schmitt Analysis, and the Cyber ‘Use-of-Force’ Debate’, *Joint Force Quarterly*, no. 67 (2012): 40; Jack Goldsmith, ‘Cybersecurity Treaties: A Skeptical View’, *Future Challenges in National Security and Law*, 2011; Lawrence T. Greenberg, Seymour E. Goodman, and Kevin J. Soo Hoo, ‘Information Warfare and International Law’ (DTIC Document, 1998); Hathaway et al., ‘The Law Of Cyber Attack’; Phillip A. Johnson, ‘An Assessment of International Legal Issues in Information Operations’ (DTIC Document, 1999); Nicholas Tsagourias, ‘Cyber Attacks, Self-Defence and the Problem of Attribution’, *Journal of Conflict and Security Law*, July 24, 2012, krs019, https://doi.org/10.1093/jcsl/krs019; Yong-Soo Eun and Judith Sita Aßmann, ‘Cyberwar: Taking Stock of Security and Warfare in the Digital Age’, *International Studies Perspectives* 17, no. 3 (2016): 343–60; Hensey A. Fenton III, ‘Proportionality and Its Applicability in the Realm of Cyber-Attacks’, *Duke Journal of Comparative & International Law* 29 (2018): 335; George R. Lucas, ‘Emerging Norms for Cyberwarfare’, *Binary Bullets: The Ethics of Cyberwarfare*, 2016, 13–33; Joseph S. Nye, ‘Nuclear Lessons for Cyber Security?’, *Strategic Studies Quarterly* 5, no. 4 (2011): 18–38; Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2 edition (Cambridge, United Kingdom ; New York, NY, USA: Cambridge University Press, 2017).
7. ‘Summary: Department of Defense Cyber Strategy 2018’ (United States Department of Defense, 2018).
8. Kristen E. Eichensehr, ‘Cyberwar & International Law Step Zero’, *Texas International Law Journal* 50, no. 2–3 (2015): 357–80; Priyanka R. Dev, ‘Use of Force and Armed Attack Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response Notes’, *Texas International Law Journal* 50, no. 2–3 (2015): 381–402.
1. William J. Lynn, \textit{Comparative Strategy} 12, no. 2 (1993): 141–65.
2. \textquote{Cyberwar Is Coming!}, \textit{Comparative Strategy} 12, no. 2 (1993): 141–65.
3. William J. Lynn, ‘Defending a New Domain: The Pentagon’s Cyberstrategy’, \textit{Foreign Affairs}, 2010, 97–108; Jason Healey, ‘A Non-State Strategy for Saving Cyberspace’, \textit{Journal of International Affairs} 70, no. 1 (2016): 13–20; Gary McGraw, ‘Cyber War Is Inevitable (Unless We Build Security In)’, \textit{Journal of Strategic Studies} 36, no. 1 (2013): 109–19.
4. Mike Orcutt, ‘Sizing Up Trump’s Cyberwar Strategy’, MIT Technology Review, March 24, 2017, \url{https://www.technologyreview.com/s/603898/sizing-up-trumps-cyberwar-strategy/}; Elias Groll, ‘Iran-Linked Hackers Said to Be Ready for Attacks on U.S. Targets’, \textit{Foreign Policy} (blog), July 1, 2019, \url{https://foreignpolicy.com/2019/07/01/iran-linked-hackers-said-to-be-ready-for-attacks-on-u-s-targets/}.
5. Richard A. Clarke and Robert Knake, \textit{Cyber War: The Next Threat to National Security and What to Do About It}, Reprint edition (New York: Ecco, 2012), 6.
6. ‘Cyberwar Is Coming!’; Hughes and Colarik, ‘The Hierarchy of Cyber War Definitions.’
7. \textit{Cyberwar, Cyberterror, Cybercrime: A Guide to the Role of Standards in an Environment of Change and Danger} (IT Governance Ltd, 2009).
8. Julie E. Mehan, \textit{CyberWar, CyberTerror, CyberCrime} (Ely: IT Governance Publishing, 2008).
9. Arquilla and Ronfeldt, ‘Cyberwar Is Coming!’
10. Sanger, \textit{The Perfect Weapon}; Healey, ‘A Non-State Strategy for Saving Cyberspace’; Nye Jr, ‘Deterrence and Dissuasion in Cyberspace’, \textit{International Security} 41, no. 3 (2017): 44–71; Hakan Mehmetcik, ‘A New Way of Conducting War: Cyberwar, Is That Real?’, in \textit{Cyberspace and International Relations} (Springer, 2014), 125–39; P. W Singer and Allan Friedman, \textit{Cybersecurity and Cyberwar: What Everyone Needs to Know}, 2014.
11. Sanger, \textit{The Perfect Weapon}; Healey, ‘A Non-State Strategy for Saving Cyberspace’; Mehmetcik, ‘A New Way of Conducting War: Cyberwar, Is That Real?’, Singer and Friedman, \textit{Cybersecurity and Cyberwar}; Healey, ‘The Spectrum of National Responsibility for Cyberattacks.’
12. Healey, ‘The Spectrum of National Responsibility for Cyberattacks’, 57.
13. Jon R. Lindsay, ‘Stuxnet and the Limits of Cyber Warfare’, \textit{Security Studies} 22, no. 3 (2013): 365–404; Michael Stohl, ‘Cyber Terrorism: A Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?’, \textit{Crime, Law and Social Change} 46, no. 4–5 (2006): 223–38.
14. Bryan Bender, ‘World More Dangerous, Top General Tells Harvard’, BostonGlobe.com, 2012, \url{https://www.bostonglobe.com/news/nation/2012/04/12/world-more-dangerous-top-general-tells-harvard-world-more-dangerous-top-general-tells-harvard/XrSM8cTzyZ0YstKv36JhJN/story.html}.
15. Gopal Ratnam and Gopal Ratnam, ‘Cybersecurity Budget up 5 Percent in 2020, White House Says’, \textit{Roll Call}, March 20, 2019, sec. whitehouse, \url{https://www.rollcall.com/news/whitehouse/cybersecurity-up-5-percent-in-2020-budget-white-house-says}; Sanger, \textit{The Perfect Weapon}.
16. Lindsay, ‘Stuxnet and the Limits of Cyber Warfare’; Alex Gibney, \textit{Zero Days}, Documentary, 2016.
17. Jerry Brito and Tate Watkins, ‘Loving the Cyber Bomb - The Dangers of Threat Inflation in Cybersecurity Policy’, \textit{Harvard National Security Journal} 3, no. 1 (2011): 39–84.
29. Thomas Rid, ‘Cyber War Will Not Take Place’, *Journal of Strategic Studies* 35, no. 1 (2012): 5–32; Jon Randall Lindsay, ‘Restrained by Design: The Political Economy of Cybersecurity’, *Digital Policy, Regulation and Governance*, 2017; Erik Gartzke, ‘Making Sense of Cyberwar’, *Policy Brief, Belfer Center for Science and International Affairs, Harvard Kennedy School*, January, 2014, 41–73.

30. Justin Joque, *Deconstruction Machines: Writing in the Age of Cyberwar* (University of Minnesota Press, 2018), chap. Introduction.

31. Lindsay, ‘Restrained by Design: The Political Economy of Cybersecurity’, 498.

32. Lindsay, 496.

33. Jerry Brito and Tate Watkins, ‘Loving the Cyber Bomb-The Dangers of Threat Inflation in Cybersecurity Policy’, 2011; Daniel E. Geer Jr, ‘Eisenhower Revisited’, *IEEE Security & Privacy*, no. 4 (2011): 88.

34. Rid, ‘Cyber War Will Not Take Place’, 2012; Thomas Rid, *Cyber War Will Not Take Place* (Oxford; New York: Oxford University Press, 2013); Lindsay, ‘Restrained by Design: The Political Economy of Cybersecurity’; Gartzke, ‘Making Sense of Cyberwar.’

35. Brandon Valeriano and Ryan Maness, ‘The Fog of Cyberwar: Why the Threat Does Not Live up to the Hype’, *Foreign Affairs*, 2012.

36. ‘Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War.’

37. Thomas Rid, *Cyber War Will Not Take Place by Thomas Rid*, 1 edition (Oxford University Press, 2013).

38. Christopher J. Finlay, ‘Just War, Cyber War, and the Concept of Violence’, *Philosophy & Technology* 31, no. 3 (September 1, 2018): 357–77, https://doi.org/10.1007/s13347-017-0299-6.

39. Timothy J. Junio, ‘How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate’, *Journal of Strategic Studies* 36, no. 1 (2013): 125–33.

40. Professor Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Reprint edition (Cambridge; New York: Cambridge University Press, 2013).

41. ‘From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik.’

42. David Whetham, ‘Cyber Chevauchees: Cyber War Can Happen’, *Binary Bullets: The Ethics of Cyberwarfare*, 2016, 86.

43. ‘The Law Of Cyber Attack.’

44. *Cyber War.*

45. *Tallinn Manual on the International Law Applicable to Cyber Warfare*; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.

46. Jose Nazario, ‘Politically Motivated Denial of Service Attacks’, *The Virtual Battlefield: Perspectives on Cyber Warfare*, 2009, 163–81.

47. Markus Sabadello, ‘The Role of New Media for the Democratization Processes in the Arab World’, *The Arab Revolutions. Reflections on the Role of Civil Society, Human Rights and New Media in the Transformation Processes*, SAFRAN Schläninger Arbeitspapiere Für Friedensforschung, Abrüstung Und Nachhaltige Entwicklung, 2011, 11.

48. Jessica L. Beyer, ‘The Emergence of a Freedom of Information Movement: Anonymous, WikiLeaks, the Pirate Party, and Iceland’, *Journal of Computer-Mediated Communication* 19, no. 2 (2014): 141–54; Robert Mackey, ‘Operation Payback’ Attacks Target MasterCard and PayPal Sites to Avenge WikiLeaks’, *New York Times*, 2010.

49. Eun and Aßmann, ‘Cyberwar: Taking Stock of Security and Warfare in the Digital Age.’

50. Clarke and Knake, *Cyber War*.

51. Clarke and Knake.

52. Healey, ‘The Spectrum of National Responsibility for Cyberattacks.’

53. Healey, 68.

54. ‘Stuxnet and the Limits of Cyber Warfare.’

55. ‘Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed’, *Journal of Strategic Studies* 35, no. 5 (2012): 689–711.
56. Alexander Klimburg, ‘Mobilising Cyber Power’, Survival 53, no. 1 (2011): 41–60; Stephen W. Korns and Joshua E. Kastenberg, ‘Georgia’s Cyber Left Hook’, Parameters 38, no. 4 (2008): 60–76; Nye Jr, ‘Deterrence and Dissuasion in Cyberspace.’

57. P. Cornish et al., ‘On Cyber Warfare’ (Chatham House, 2012); Nye Jr, ‘Deterrence and Dissuasion in Cyberspace’; Manjikian, ‘From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik’; Healey, ‘A Non-State Strategy for Saving Cyberspace’; Fenton III, ‘Proportionality and Its Applicability in the Realm of Cyber-Attacks’; Jon R. Lindsay and Erik Gartzke, ‘Coercion through Cyberspace: The Stability-Instability Paradox Revisited’, in Coercion: The Power to Hurt in International Politics, ed. Kelly Greenhill and Peter Krause (Oxford University Press, 2018).

58. Lucas, ‘Emerging Norms for Cyberwarfare’, 18.

59. Erik Gartzke, ‘The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth’, International Security 38, no. 2 (2013): 41–73; Lindsay, ‘Restrained by Design: The Political Economy of Cybersecurity’; Angelyn Flowers and Sherali Zealdally, ‘Cyberwar: The What, When, Why, and How’, IEEE Technology and Society Magazine 33, no. 3 (2014): 14–21; Markus Christen and Endre Bangerter, ‘Is Cyberpeace Possible?’, in The Nature of Peace and the Morality of Armed Conflict (Springer, 2017), 243–63; Rid, ‘Cyber War Will Not Take Place’, 2012; Christopher M. Sanders, ‘The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an Act of War Note’, Utah Law Review 2018, no. 2 (2018): i–522; Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations; Lindsay and Gartzke, ‘Coercion through Cyberspace: The Stability-Instability Paradox Revisited’; Healey, ‘The Spectrum of National Responsibility for Cyberattacks’; ‘Summary: Department of Defense Cyber Strategy 2018’; Louise Arimatsu, ‘Classifying Cyber Warfare’, in Research Handbook on International Law and Cyberspace (Edward Elgar Publishing, 2015); Nye, ‘Nuclear Lessons for Cyber Security?’

60. Roland Heickerö, Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations, 2010; Matthew Mowthorpe, ‘The Revolution in Military Affairs (RMA): The United States, Russian and Chinese Views’, The Journal of Social, Political, and Economic Studies 30, no. 2 (2005): 137.

61. Molly Sauter and Ethan Zuckerman, The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet (New York: Bloomsbury Academic, 2014); Leandro Oliva, ‘Is DDoS the New ‘Sit-In’?’, Motherboard, 2013, http://motherboard.vice.com/blog/is-ddos-the-new-civil-disobedience; Council of Europe, ‘Report by the Committee of Experts on Cross-Border Flow of Internet Traffic and Internet Freedom on Freedom of Assembly and Association on the Internet’ (Council of Europe, December 10, 2015).

62. Ralph Langner, ‘Stuxnet’s Secret Twin’, Foreign Policy (blog), 2013, https://foreignpolicy.com/2013/11/19/stuxnets-secret-twin/.

63. Healey, ‘The Spectrum of National Responsibility for Cyberattacks.’

64. Clarke and Knake, Cyber War.

65. ‘Cyber War Will Not Take Place’, 2012; Cyber War Will Not Take Place, 2013.

66. Sanger, The Perfect Weapon.

67. Valeriano and Maness, ‘The Fog of Cyberwar: Why the Threat Does Not Live up to the Hype’; Martin C. Libicki, ‘Cyberspace Is Not a Warfighting Domain’, IJS: A Journal of Law and Policy for the Information Society 8 (2012): 321.

68. Michael V. Hayden, ‘The Future of Things Cyber’, Strategic Studies Quarterly 5, no. 1 (2011): 3–7.

69. Clarke and Knake, Cyber War; Sanger, The Perfect Weapon; Healey, ‘A Non-State Strategy for Saving Cyberspace.’

70. Valeriano and Maness, ‘The Fog of Cyberwar: Why the Threat Does Not Live up to the Hype’; Joque, Deconstruction Machines: Writing in the Age of Cyberwar; Gartzke, ‘The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth.’

71. Samuel P. Huntington, ‘The Clash of Civilizations?’, Foreign Affairs, 1993, 22–49; Brito and Watkins, ‘Loving the Cyber Bomb—The Dangers of Threat Inflation in Cybersecurity Policy’; Sean Lawson, ‘Putting the ‘War’ in Cyberwar: Metaphor, Analogy, and Cybersecurity
Discourse in the United States’, First Monday 17, no. 7 (June 18, 2012), http://ojs-prod-lib.cc.uic.edu/ojs/index.php/fm/article/view/3848.

72. John Arquilla, ‘Twenty Years of Cyberwar’, Journal of Military Ethics 12, no. 1 (April 1, 2013): 80–87, https://doi.org/10.1080/15027570.2013.782632.

73. Clarke and Knake, Cyber War; Healey, ‘A Non-State Strategy for Saving Cyberspace’; Singer and Friedman, Cybersecurity and Cyberwar; Sanger, The Perfect Weapon.

74. Healey, ‘A Non-State Strategy for Saving Cyberspace’; Nye Jr, ‘Deterrence and Dissuasion in Cyberspace.’

75. James Stavridis and Dave Weinstein, ‘The Internet of Things Is a Cyberwar Nightmare’, Foreign Policy (blog), November 3, 2016, https://foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/.

76. Clarke and Knake, Cyber War; Healey, ‘The Spectrum of National Responsibility for Cyberattacks.’

77. Daniel K. Rosenfield, ‘Rethinking Cyber War’, Critical Review 21, no. 1 (2009): 77–90, https://doi.org/10.1080/08913810902812156.

78. Siobhan Forman and Julian E. Barnes, ‘Cyber-Combat: Act of War—Pentagon Sets Stage for US to Respond to Computer Sabotage with Military Force’, Wall Street Journal 30 (2011); Sanger, The Perfect Weapon.

79. Brito and Watkins, ‘Loving the Cyber Bomb—The Dangers of Threat Inflation in Cybersecurity Policy’; Clay Wilson, ‘Cyber Threats to Critical Information Infrastructure’, in Cyberterrorism (Springer, 2014), 125–36.

80. James Adams, ‘Virtual Defense’, Foreign Affairs, 2001, 98–112; John Arquilla, ‘Cyberwar Is Already upon Us’, Foreign Policy 192 (2012); Arquilla and Ronfeldt, ‘Cyberwar Is Coming’!

81. Chairman of the Joint Chiefs of Staff, Joint Publication JP 3-27 Homeland Defense 29 July 2013 (CreateSpace Independent Publishing Platform, 2013), III–15.

82. Daniel T. Kuehl, ‘From Cyberspace to Cyberpower: Defining the Problem’, Cyberpower and National Security, 2009, 26–28.

83. M. C. FitzGerald, ‘Russian Views on Electronic and Information Warfare’, in Proceedings of the Third International Command and Control Research and Technology Symposium: Partners for the 21st Century, National Defense University, vol. 126, 1997; Timothy L. Thomas, ‘The Russian View Of Information War’, The Russian Armed Forces at the Dawn of the Millennium, 2000, 335; Warner, ‘Cybersecurity: A Pre-History.’

84. William Jefferson Clinton, ‘Executive Order 13010—Critical Infrastructure Protection’, Federal Register 61, no. 138 (1996): 37347–50; Eric Talbot Jensen, ‘Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defense’, Stanford Journal of International Law 38 (2002): 207; John Moteff and Paul Parfomak, ‘Critical Infrastructure and Key Assets: Definition and Identification’ (DTIC Document, 2004); Healey, ‘A Non-State Strategy for Saving Cyberspace.’

85. ‘The Territorial Trap: The Geographical Assumptions of International Relations Theory.’

86. Adams, ‘Virtual Defense’; Christopher C. Joyner and Catherine Lotrionte, ‘Information Warfare as International Coercion: Elements of a Legal Framework’, European Journal of International Law 12, no. 5 (2001): 825–65.

87. Delibasis, The Right to National Self-Defense: In Information Warfare Operations; Rid, ‘Cyber War Will Not Take Place’, 2012.

88. Rid, ‘Cyber War Will Not Take Place’, 2012.

89. Ronald Deibert, Black Code: Surveillance, Privacy, and the Dark Side of the Internet (Toronto: Signal, 2013).

90. Deibert.

91. Omry Haizler, ‘The United States’ Cyber Warfare History: Implications on Modern Cyber Operational Structures and Policymaking’, Cyber, Intelligence, and Security 1, no. 1 (2017): 31–45.

92. Joque, Deconstruction Machines: Writing in the Age of Cyberwar.

93. Finlay, ‘Just War, Cyber War, and the Concept of Violence’; Rid, ‘Cyber War Will Not Take Place’, 2012; Joque, Deconstruction Machines: Writing in the Age of Cyberwar; Valeriano and
Maness, ‘The Fog of Cyberwar: Why the Threat Does Not Live up to the Hype’; Gartzke, ‘The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth’; Brandon Valeriano and Ryan C. Maness, Cyber War versus Cyber Realities: Cyber Conflict in the International System (Oxford University Press, USA, 2015).

94. Rosenfield, ‘Rethinking Cyber War’; Thomas Rid and Ben Buchanan, ‘Attributing Cyber Attacks’, Journal of Strategic Studies 38, no. 1–2 (January 2, 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

95. Rid, ‘Cyber War Will Not Take Place’, 2012; Rid, Cyber War Will Not Take Place, 2013; Rosenfield, ‘Rethinking Cyber War’.

96. Rid, ‘Cyber War Will Not Take Place’, 2013; Rid, ‘Cyber War Will Not Take Place’, 2012; Sanger, The Perfect Weapon; Healey, ‘The Spectrum of National Responsibility for Cyberattacks’.

97. Klimburg, ‘Mobilising Cyber Power’.

98. Morozov, ‘Battling the Cyber Warmongers’.

99. Evgeny Morozov, ‘Battling the Cyber Warmongers’, The Wall Street Journal 8 (2010).

100. Rosenfield, ‘Rethinking Cyber War’.

101. Rosenfield.

102. Valeriano and Maness, Cyber War versus Cyber Realities: Cyber Conflict in the International System.

103. Joque, Deconstruction Machines: Writing in the Age of Cyberwar; Finlay, ‘Just War, Cyber War, and the Concept of Violence’; William Merrin and Andrew Hoskins, ‘Tweet Fast and Kill Things: Digital War’, Journal of Digital War, March 17, 2020, https://doi.org/10.1057/s42984-020-00002-1; Tim Stevens, ‘Knowledge in the Grey Zone: AI and Cybersecurity’, Journal of Digital War, March 31, 2020, https://doi.org/10.1057/s42984-020-00007-w.

104. T. Michael Moseley, ‘The Nation’s Guardians: America’s 21st Century Air Force’ (DTIC Document, 2007); Gregory J. Rattray, Strategic Warfare in Cyberspace (MIT press, 2001); James Yin and Philip M. Taylor, ‘Information Operations from an Asian Perspective: A Comparative Analysis’, Journal of Information Warfare 7, no. 1 (2008): 1–23; Bruce D. Berkowitz, The New Face of War: How War Will Be Fought in the 21st Century, First Edition edition (New York: Free Press, 2003).

105. Morozov, ‘Battling the Cyber Warmongers’, 2010.

106. Michael Joseph Gross, ‘A Declaration of Cyber-War’, Vanity Fair 53 (2011).

107. Rose McDermott, ‘Some Emotional Considerations in Cyber Conflict’, Journal of Cyber Policy 4, no. 3 (September 2, 2019): 309–25, https://doi.org/10.1080/23738871.2019.1701692.

108. Klimburg, ‘Mobilising Cyber Power’; Craig B. Greathouse, ‘Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?’, in Cyberspace and International Relations: Theory, Prospects and Challenges, ed. Jan-Frederik Kremer and Benedikt Müller (Berlin, Heidelberg: Springer Berlin Heidelberg, 2014), 21–40, https://doi.org/10.1007/978-3-642-37481-4_2.

109. Evgeny Morozov, ‘Battling the Cyber Warmongers’, Wall Street Journal, May 8, 2010, sec. Life and Style, https://www.wsj.com/articles/SB10001424052748704370704575228653351323986.

110. ‘Cyber War Will Not Take Place’, 2012.

111. Rid.

112. Thomas Rid, ‘Think Again: Cyberwar’, Foreign Policy (blog), 2012, http://foreignpolicy.com/2012/02/27/think-again-cyberwar/; Bruce Schneier, ‘Threat of ‘cyberwar’ Has Been Hugely Hyped - CNN.Com’, 2010, http://www.cnn.com/2010/OPINION/07/07/schneier.cyberwar.hyped/; The Economist, ‘Hype and Fear’, The Economist, December 8, 2012, http://www.economist.com/news/international/21567886-america-leading-way-developing-doctrines-cyber-warfare-other-countries-may.

113. Tom Gjelten, ‘Is All The Talk About Cyberwarfare Just Hype?’, NPR.org, 2013, http://www.npr.org/2013/03/15/174352914/is-all-the-talk-about-cyberwarfare-just-hype.
114. Manjikian, ‘From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik.’
115. Mark Nunes, ‘Distributed Terror and the Ordering of Networked Social Space’, *Media/ Culture Journal* 7, no. 6 (2005): 1–3; Whetham, ‘Cyber Chevauchees: Cyber War Can Happen’; Fenton III, ‘Proportionality and Its Applicability in the Realm of Cyber-Attacks’; Eun and Aßmann, ‘Cyberwar: Taking Stock of Security and Warfare in the Digital Age’; Nye, ‘Nuclear Lessons for Cyber Security?’; Lucas, ‘Emerging Norms for Cyber-warfare’; Sai Felicia Krishna-Henzel, ‘Cybersecurity: Perspectives on the Challenges of the Information Revolution’, *Power and Security in the Information Age. Investigating the Role of the State in Cyberspace*. Burlington: Ashgate, 2007.
116. William Yurcik, ‘Information Warfare: Legal & Ethical Challenges of the next Global Battleground’, in *Proceedings of the 2nd Annual Ethics and Technology Conference (Ethics’ 97)*. Loyola University Chicago (Citeseer, 1997).
117. Michael Robinson, Kevin Jones, and Helge Janicke, ‘Cyber Warfare: Issues and Challenges’, *Computers & Security* 49 (2015): 70–94.
118. Irving Lachow and Courtney Richardson, ‘Terrorist Use of the Internet: The Real Story’ (DTIC Document, 2007); Nunes, ‘Distributed Terror and the Ordering of Networked Social Space’; Lindsay, ‘Restricted by Design: The Political Economy of Cybersecurity’; Lindsay and Gartzke, ‘Coercion through Cyberspace: The Stability-Instability Paradox Revisited.’
119. Moseley, ‘The Nation’s Guardians: America’s 21st Century Air Force.’
120. Robinson, Jones, and Janicke, ‘Cyber Warfare: Issues and Challenges.’
121. Lucas, ‘Emerging Norms for Cyberwarfare.’
122. Alan D. Campen, Douglas H. Dearth, and R. Thomas Goodden, *Cyberwar: Security, Strategy, and Conflict in the Information Age* (AFCEA International Press Fairfax, VA, 1996); Moseley, ‘The Nation’s Guardians: America’s 21st Century Air Force.’
123. Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology*, 1st ed. (University Of Chicago Press, 1989).
124. John A. Nagl et al., *The US Army/Marine Corps Counterinsurgency Field Manual* (University of Chicago Press, 2008); Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
125. Mark Milone, ‘Hakactivism: Securing the National Infrastructure’, *Knowledge, Technology & Policy* 16, no. 1 (2003): 75–103; Rattray, *Strategic Warfare in Cyberspace*; Fenton III, ‘Proportionality and Its Applicability in the Realm of Cyber-Attacks’; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.
126. Libicki, ‘Cyberspace Is Not a Warfighting Domain.’
127. Moseley, ‘The Nation’s Guardians: America’s 21st Century Air Force’; ‘Summary: Department of Defense Cyber Strategy 2018.’
128. Peter Pascucci, ‘Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution’, *Minnesota Journal of International Law* 26 (2017): 419.
129. Barkham, ‘Information Warfare and International Law on the Use of Force’; Greenberg, Goodman, and Soo Hoo, ‘Information Warfare and International Law’; Hathaway et al., ‘The Law Of Cyber Attack’; Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*; Fenton III, ‘Proportionality and Its Applicability in the Realm of Cyber-Attacks.’
130. Sanger, *The Perfect Weapon*.
131. Robert Kaiser, ‘The Birth of Cyberwar’, *Political Geography* 46 (2015): 11–20.
132. Argyro P. Karanasiou, ‘The Changing Face of Protests in the Digital Age: On Occupying Cyberspace and Distributed-Denial-of-Services (DDoS) Attacks’, *International Review of Law, Computers & Technology* 28, no. 1 (2014): 98–113; Sauter and Zuckerman, *The Coming Swarm*; Oliva, ‘Is DDoS the New ‘Sit-In’?’; Council of Europe, ‘Report by the Committee of Experts on Cross-Border Flow of Internet Traffic and Internet Freedom on Freedom of Assembly and Association on the Internet.’
133. Lillian Ablon and Andy Bogart, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (Rand Corporation, 2017).

134. Marie Baezner, ‘Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions’ (ETH Zurich, 2019).

135. Rosenfield, ‘Rethinking Cyber War.’

136. Healey, ‘The Spectrum of National Responsibility for Cyberattacks’, 57.

137. Sanger, *The Perfect Weapon*.

138. Michael Joseph Gross, ‘Silent War’, *Vanity Fair*, 2013; Baezner, ‘Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions’; David E. Sanger and Nick Corasaniti, ‘D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump’, *The New York Times*, June 14, 2016, sec. U.S., https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html.

139. Peter Foster, ‘Bogus’ AP Tweet about Explosion at the White House Wipes Billions off US Markets’, *Telegraph.Co.Uk*, 2013, sec. markets, http://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html.

140. Sanger, *The Perfect Weapon*; Baezner, ‘Iranian Cyber-Activities in the Context of Regional Rivalries and International Tensions.’

141. Richard J. Harknett and Max Smeets, ‘Cyber Campaigns and Strategic Outcomes’, *Journal of Strategic Studies*, March 4, 2020, 25, https://doi.org/10.1080/01402390.2020.1732354.

142. Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance (Information Revolution and Global Politics)* (The MIT Press, 2009).

143. ‘Summary: Department of Defense Cyber Strategy 2018’, 4.

144. Klimburg, ‘Mobilising Cyber Power’; ‘Summary: Department of Defense Cyber Strategy 2018.’

145. Rebecca Smith and Rob Barry, ‘America’s Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It’, *Wall Street Journal*, January 10, 2019.

146. David E. Sanger and Nicole Perlroth, ‘U.S. Said to Find North Korea Ordered Cyberattack on Sony’, *The New York Times*, December 17, 2014, http://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

147. Sanger, *The Perfect Weapon*.

148. Robinson, Jones, and Janicke, ‘Cyber Warfare: Issues and Challenges’; Hughes and Colarik, ‘The Hierarchy of Cyber War Definitions.’

149. Hughes and Colarik, ‘The Hierarchy of Cyber War Definitions’.

**Disclosure statement**

No potential conflict of interest was reported by the author(s).

**Notes on contributor**

*Cameran Ashraf* is assistant professor of new media and global communications at the School of Public Policy, Central European University, and co-founder of AccessNow, one of the largest international human rights organisations dedicated to defending human rights in the digital age. Based on his work, the European Parliament selected AccessNow as finalist for the 2010 Sakharov Prize for Freedom of Thought, the European Union’s highest human rights honour.