
NEW AMERICA
CYBERSECURITY INITIATIVE
JAMES SHIRES AND MAX SMEETS
CONTESTING "CYBER"
DECEMBER 2017

About the Authors

James Shires is a doctoral student in international relations at the University of Oxford, and a research affiliate at the Oxford Center for Technology and Global Affairs. His research focuses on cybersecurity in the Middle East.

Max Smeets is a postdoctoral scholar at CISAC at Stanford University. He is also a fellow in New America's Cybersecurity Initiative. He holds a DPhil in international relations from the University of Oxford, St. John's College.

Acknowledgements

We thank Jamie Collier, Kjølv Egeland, Florian Egloff, and Robert Morgus for their comments on an earlier draft of this report.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring New America's focus on big ideas, bringing together technology and policy, and public engagement to the cybersecurity conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. A collaboration between New America's Open Technology Institute and International Security program, our work explores important cybersecurity policy questions at all levels of government and policy making, from the state and local to national and international. Examining issues from the vulnerabilities equities process in governments and the importance of cybersecurity policy at the state and local level to the potential of strong and stable international regimes to promote better cybersecurity, New America's Cybersecurity Initiative seeks to address issues others can't or don't and create impact at scale.

Our work is made possible through the generous support of the Florida International University, the William and Flora Hewlett Foundation, Microsoft Corporation, the Government of the United Kingdom, Endgame Inc., and the MITRE Corporation.

Find out more: **newamerica.org/cybersecurity-initiative**

Contents

Introduction	2
Cyber: Not Just a Confused but also a Contested Concept	3
The Connotations of “Cyberspace” Shift from Opportunity to Threat	4
Substantive vs. Implied Definitions: A Mundane Stuff or the Wild West?	6
“Cyber-Exceptionalism”	7
ARPANET: Where Did it all Start Again?	8
Exit, Voice, and Cyberspace	10
Discussion	11
Notes	12

INTRODUCTION

Over the last few decades there has been a proliferation of the term "cyber," and commensurate levels of inconsistency.* This report argues that the inconsistent application of the prefix "cyber" stems not only from confusion, as some scholars and policymakers have proposed, but also from contest. Our goal is not to resolve conceptual disputes, but instead to understand how and why contests have occurred, and whether resolution is possible.

As the prefix "cyber" has rarely been used alone, we place the concept of cyberspace at the center of analysis, for two reasons. First, it is often considered to be the most basic concept in the field, drawing on an intuitive geographical metaphor. Second, "cyberspace" can be considered a least-likely (or least-obvious) study of contest. The attachment of the prefix "cyber" to various nouns has left cyber-related concepts with a variety of underlying normative connotations. On one side, some cyber-related concepts are *prima facie* undesirable, like "cyber warfare" or "cyber threat." Others are more positive, such as "cyber democracy." The obvious normative aspects of the terms to which the cyber prefix is attached make these likely sites for contest, whereas "cyberspace" is seemingly more neutral. We suggest instead that it is the ominous calm at the heart of the storm, providing an excellent case in which to study the tension regarding the prefix more broadly.

This report argues that cyberspace is contested in several ways: through a change in connotations from opportunity to threat, through the existence of substantive and implied definitions with different rhetorical functions, and through competing understandings of the key historical exemplar for cyberspace, that of ARPANET. We conclude that, as the prospects for agreement regarding cyberspace are low, we should adopt what we term, following Hirschman, an 'exit' rather than 'voice' strategy, and use other concepts instead.

*This report is a compilation of blog posts published on the New America website, read part one here: https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/contesting-cyber/

CYBER: NOT JUST A CONFUSED BUT ALSO A CONTESTED CONCEPT

Since the early 1990s the prefix "cyber" has become widespread. As often noted, its use stretches back to Norbert Wiener's coinage of "cybernetics" from its Greek equivalent in the 1940s. It is similarly canonical to cite novelist William Gibson as creating the "ur" metaphor for this prefix in the early 1980s by combining it with "space." Almost three decades later, in an interview with the A.V. Club, Gibson argued that "'cyberspace' as a term is sort of over. It's over in the way that after a certain time, people stopped using the prefix '-electro' to make things cool, because everything was electrical. 'Electro' was all over the early twentieth century, and now it's gone. I think 'cyber' is sort of the same way."

In contrast to Gibson's prediction, a simple automated content analysis using Google Trends indicates that the popularity of the prefix "cyber" has remained stable (with a spike in November each year for "cyber Monday"). There are ever more applications of this prefix, to words such as crime, law, cafe, hate, bullying, attack, war, vandalism, politics, dating, security, and power. Today, more people enter the search term "cyber" into Google than the term "democracy" or "terrorist." Needless to say, the term "cyber" has also gained in prominence in academia and policymaking.

The proliferation of this prefix has, inevitably, led to substantial inconsistencies in its use. On one level, these contradictions may stem from simple confusion. As Michael Hayden, former director of the CIA and NSA, remarked: "rarely has something been so important and so talked about with less clarity and apparent understanding than this phenomenon." Scholars and policymakers, among others, are not always consistent in their own usage of cyber-related concepts, and they sometimes reinterpret the definitions employed by others, especially when given a liberal dose of cross-disciplinary fertilization.

Influential voices have suggested that such confusion is primarily caused by the apparently abstruse and multifaceted nature of the phenomenon. For example, in a Foreign Policy article, Stephen Walt notes that "the whole issue is highly esoteric—you really need to know a great deal about computer networks, software, encryption, etc., to know how serious the danger might be," concluding that "here are lots of different problems being lumped under a single banner, whether the label is 'cyber-terror' or 'cyber-war'." If this were the case, more research would iron out the lack of clarity surrounding this relatively young concept, and then we can get to *the* one and only "meaning of the cyber revolution," as Lucas Kello emphasizes in his recent book (and earlier article).

However, in this report we argue that the inconsistent application of the prefix "cyber" stems not only from confusion, but also from *contestation*.

In other words, the roots of disagreement are deeper than a mere struggle to absorb the collective knowledge of varied disciplines, but stem from underlying normative disagreements.

Understanding the nature and extent of this contestation of "cyber" is important for both policymaking and academic research. For policymakers, the promise of what Joseph Nye Jr. calls "rules of the road" in cyberspace is much diminished if the very domain itself remains in question. Constructing effective international cyber-governance becomes more difficult—although not impossible—if the scope of what to be governed is fundamentally disputed.

For academics, if the roots of disagreement are deeper, then faith in a unified understanding of the cyber-issue is utopic; and further investigation of why and how broader political disputes are translated into problems with this proliferating prefix is urgently required.

Here we will explore what it means when we talk about cyber, and address the nature of contestation from five separate angles.

THE CONNOTATIONS OF "CYBERSPACE" SHIFT FROM OPPORTUNITY TO THREAT

In many early uses of the term, cyberspace had clear connotations of achievement or approval. Here, cyberspace reflected a sense of progress and modernity, a new step in history. In the words of Patricia Aufderheide, writing in the late 90s, "[c]yberspace is the land of knowledge, and the exploration of that land can be a civilization's truest, highest calling. The opportunity is now before us to empower every person to pursue that call in his or her own way."

It is important to distinguish this general sense of positivity from individual arguments that cyberspace will bring certain benefits, although they are linked. For example, the expansion of cyberspace has often been associated with the advancement of democracy, and many consultancy reports list the economic benefits cyberspace can bring. On their own, these uses of "cyberspace" do not create connotations of opportunity and possibility. That occurs when the overall weight of such articles—the discourse around cyberspace—

connects it to democracy, freedom, economic benefits, increased social interaction, and other values so closely that the very mention of cyberspace implies these various positive notions, and so it adopts a note of achievement of its own.

However, this view of its benefits has, in more recent years, been tempered with the recognition that it is "a dangerous world"; what Ronald Deibert calls the "dark side of cyberspace." While the potential perils of new technologies were never far from the surface in popular culture, cyberspace from this perspective *primarily* means new threats, most principally cyber crime, cyber war, and potentially cyber terrorism. As with the more positive uses above, it is important to note that in this respect individual threats in cyberspace do not make it a wholly insecure space; rather, it is the combined weight of many of those threats that gives the *concept* of cyberspace itself such connotations.

While the potential perils of new technologies were never far from the surface in popular culture, cyberspace from this perspective primarily means new threats, most principally cyber crime, cyber war, and potentially cyber terrorism.

Of course, many treatments of cyberspace include references to both risks and opportunities, recognizing (and providing further fuel for) both connotations. Nonetheless, some authors discern a pattern to changes in the connotations of cyberspace. Namely, that there has been a "colonization" of the term by military/security communities, in the United States in particular. Bendrath, Dunn Cavelty, and Hansen and Nissenbaum among others, all demonstrate the "securitization" of cyberspace in this manner. While Bendrath and Dunn Cavelty both focus on U.S. government discourse, Hansen and Nissenbaum focus instead on the global response to the Estonia incident in 2007, demonstrating that this is a wider phenomenon.

To illustrate this work, we provide a brief example from the U.S. policy world, examining the Brookings Institution, an influential U.S. policy organization. The Brookings Institution published six documents on cyberspace before 2000, and none of these articles focused on the security implications (instead the article are about commerce, elections, and tax dodging and communication). From 2000 to 2011, this focus shifted, as of the fifteen articles on cyberspace, eleven were on security and military implications. This shift then dramatically increased. When one searches "cyber" on the Brookings website, no more than five of the 77 results published between January 1, 2011 and January 1, 2016 focus on something other than securing against the threat from cyberspace.

Finally, one can connect this shift in the connotations of cyberspace to its real-world consequences. Several authors, including Robert M. Lee and Thomas Rid, have suggested that the "cyber" prefix is used to generate hype, especially in the military/security community. This hype makes it easier to access financial resources for new initiatives. The brief overview of the securitization of cyberspace above takes this suggestion further. Not only do various public and private actors use the "cyber" prefix for political and financial gain in both security and non-security sectors, as Lee and Rid suggest, but this activity changes the concept itself. There is therefore a feedback loop between hyped uses of "cyber" and "cyberspace," and a shift in the *meaning* of the concept from opportunity to threat.

SUBSTANTIVE VS. IMPLIED DEFINITIONS: A MUNDANE STUFF OR THE WILD WEST?

Descriptions of cyberspace can be split into two main types: substantive and implied. The former create a meaning for cyberspace by saying what it is, while the latter say what it is not. Often these two descriptions intermingle, but they just as often stand alone as sufficient for displaying the meaning of the concept. We suggest that these two types of descriptions have different rhetorical functions, which assist the contest over cyberspace.

Substantive descriptions include several well-known academic definitions. In Lucas Kello's view cyberspace comprises "(1) the internet, encompassing all interconnected computers, including (2) the world wide web, consisting only of nodes accessible via a URL interface; and (3) a cyber 'archipelago' comprising all other computer systems that exist in theoretical seclusion." Martin Libicki writes that cyberspace consists of three separate but interconnected layers: the physical layer, consisting of computer systems and wires; the syntactic layer, the instructions and protocols established by the designers and users; and the semantic layer, the contained information.

Implied descriptions of cyberspace focus on what is absent, rather than enumerating its content or layers. Here cyberspace is defined by implication, as a place without law, borders, government, location, physical structures, states, or identity. From a legal perspective, Johnson and Post suggest that it is intrinsic to cyberspace that it "has no territorially based boundaries [...] The power to control activity in cyberspace has only the most tenuous connections to physical location." In international relations, Rid and Buchanan have pointed out that the difficulty of attribution is often thought to be a defining characteristic of cyberspace. From another discipline altogether, Lal writes that "cyberspace has no precise physical location, no singular identity." The implied attributes are not necessarily negative. Many implied definitions of cyberspace point to its lack of bureaucracy, geographical limitations, or biases and prejudices based on physical presence.

We suggest that substantive and implied definitions of cyberspace are not merely the statement of different facts, but are also types of rhetoric: the use of language and style to persuade audiences of a particular point of view. In an oratory tradition stretching back to Cicero, the strategic setting of ground for debate is a key rhetorical move, and one cannot start earlier than a definition of the object of study itself.

If one wants to produce substantive knowledge about a specific topic, there is a feeling of comfort provided by the enumeration of the features of cyberspace. In contrast, if one is aiming to provoke decision and action, then what is required is exactly the opposite. In that case, one wants to create a feeling of discomfort to show that cyberspace is not anything like the land you thought you knew, and therefore steps must be taken to control it, to tame it. This is where the implied definitions are at their most powerful.

"CYBER EXCEPTIONALISM"

In this section we argue that the concept of cyberspace enables a form of exceptionalism, similar to "American exceptionalism." Though American exceptionalism is said to lack a formal definition, resting on a cluster of stories, it is normally used to describe the notion that the United States embodies a unique national culture with a shared purpose. There is also a sense that, once settled in the City upon a Hill, one will inevitably start to internalize these unique culture and ideals.

In cyberspace, cyber exceptionalism suggests a similar distinctiveness of culture, approach, and even tactics and strategy. Cyber exceptionalism is the process by which the application of the prefix "cyber" to any concept x, such as space, thereby opens up an analytical difference between the meaning of cyber-x and x.

In *A Declaration of the Independence of Cyberspace*, techno-libertarian John Perry Barlow wrote, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. [...] We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks."

Barlow's *Declaration* was widely distributed after it was published online on February 8, 1996, receiving both praise and critique. As we have noted, we can distinguish between two types of definitions of cyberspace: substantive and implied. Barlow set out an implied definition of cyberspace to create this sense of cyber exceptionalism.

Over time, cyber exceptionalism has grown into a conceptual strategy as well as a culture. In early November 2017, about 40 scholars and policymakers gathered at Columbia University for the "Bridging the Gap Workshop." The first session concerned a

whiteboard exercise on "conceptualizations of cyber conflict." Participants were asked to split up in groups and define terms such as "cyber deterrence," "cyber coercion," "cyber diplomacy," and "cyber compellence." After about 30 minutes, each group came back and reported on the unique features of each term. In this setting, replicated across universities, governments, and think tanks, cyber exceptionalism is a basic assumption, structuring the thinking of those tackling "cyber" issues.

The idea of cyber exceptionalism is important for those advocating that "cyber" questions require an entirely separate approach. Just as the discipline of international relations came into being because the international system was perceived to be fundamentally different from domestic society, at the core of cyber exceptionalism is the belief that the growth of cyberspace creates distinct dynamics worthy of placing into a new field of study.

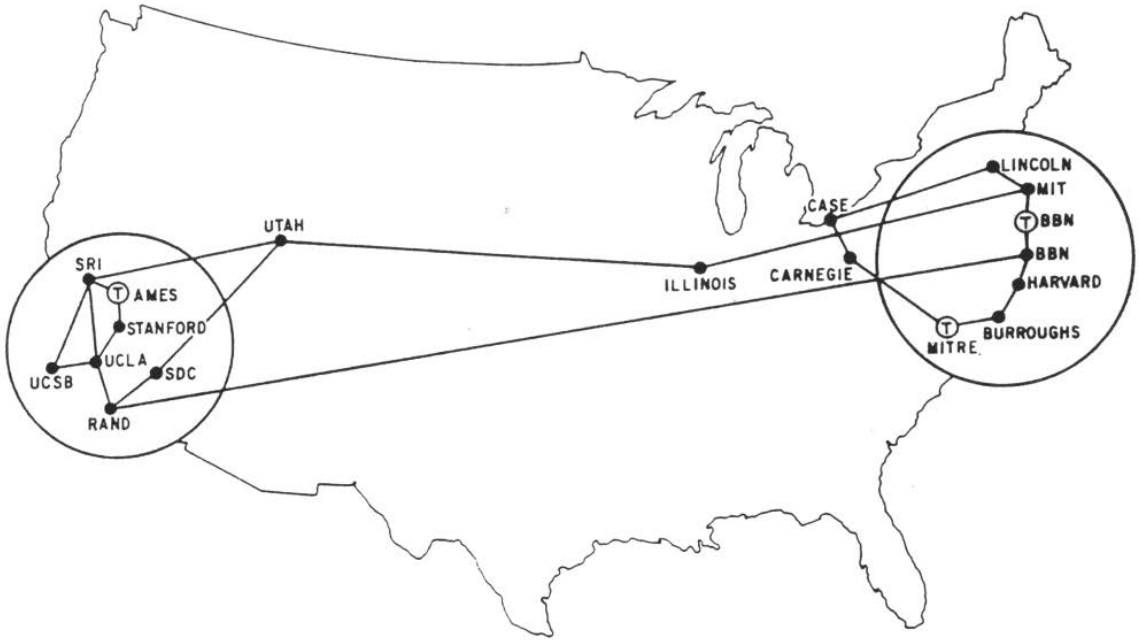
ARPANET: WHERE DID IT ALL START AGAIN?

There is said to be a single hook around which much of the scholarship on cyberspace evolved. This is ARPANET, which was implemented in October 1969 when four university computers became interconnected in the United States. ARPANET serves both as an anchor point for explaining what cyberspace once was as well as way of expounding the principles underlying cyberspace today.

Yet, there are still multiple ways of describing this foundational project. From one perspective, ARPANET is taken to reveal that cyberspace has always been a tool for political power struggles. According to Roger Hurwitz, "[e]ven liberal regimes have sought power to police cyberspace... [later] struggles uncannily rewrite in large those earlier tensions when the federal government owned ARPANET and researchers fretted that their using it for personal communications might run afoul of the overseers."

For others, ARPANET is mainly proof that the military has always been interested and involved in cyberspace from the very beginning. It is often pointed out that the DARPA funded community—with J.C.R Licklider as the first head of the computer research program and Ivan Sutherland, Bob Taylor, and Lawrence G. Roberts as his successors—was indeed at the birth of ARPANET. Also one of the

Figure 1 | ARPANET, September 1971



Source: Chiappa, J. Noel. "ARPANET Technical Information: Geographic Maps, September, 1971." http://mercury.lcs.mit.edu/~jnc/tech/arpageo.html

goals of ARPANET was to design a decentralized network which could continue even in case networks were damaged.

Yet the feature which is most frequently emphasized is that ARPANET was largely considered an academic project, with trust and availability trumping security. Raphael Cohen-Almagor writes, "the culture of the ARPANET community was one of open research, free exchange of ideas, no overbearing control structure, and mutual trust."

Similarly, Joseph Nye Jr. states, "ARPANET [...] [was] essentially a research tool and the plaything of a few. In other words, the massive vulnerabilities that have created the security problems we face today are less than two decades old and are likely to increase."

Overall, existence of different descriptions for the same foundational project, ARPANET, is thus another means of contest for the concept of cyberspace.

EXIT, VOICE, AND CYBERSPACE

Albert Hirschman, in his classic work *Exit, Voice, and Loyalty*, states that in declining firms, organizations or states can either "exit"—i.e. withdraw from the relationship— or use their "voice"—i.e. try to repair the relationship by speaking out in favor of change. Whereas the latter is visible and at times confrontational, the former type of action is more difficult to detect. Indeed, "exit" is often associated with Adam Smith's Invisible Hand, in which the market automatically (and silently) channels self-interest toward socially desired outcomes.

Where previous sections have considered how different uses of "cyberspace" are recognized (or not) by various camps, our view is that there is also an equivalent of Hirshmann's "exit and voice" strategy in conceptual contestation.

Contesting the meaning of cyberspace, as examined above, is the equivalent of "voice." Yet, this is only one half of the story. There is also contest in this area through the *lack of use*. This means that we not only have to look at the different uses of the word "cyber" or "cyberspace," but we also have to understand how it is used vis-à-vis other words that operate in similar semantic terrain, such as "digital," "internet," "electronic," and so on.

For example, some have shied away from using the term "cyber democracy" but instead talk about "e-democracy" or "digital-democracy." Likewise, the United Nations GGE does not actually mention cyber in its name; its long-hand title is "the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." It was initially created in response to a Russian request for state cooperation in 1998 on information security, but collapsed in June 2017 over differences in the applicability of international law "in cyberspace."

Further, the Chinese and Russian governments tend to refer to "information space," while references to "cyberspace" occur primarily in translations of foreign works. A similar difference can be found in Arabic, where "cybersecurity" is often translated as *al-'amn al-raqmi* (digital security) or *'amn al-mu'alumat* (information security), as well as using the loan word *al-'amn al-sibrani* (cybersecurity). These varied translation choices for the cyber prefix facilitate exit in regions where English is not the only language, as they provide further scope for reinterpretation.

As Hirschman notes, the interplay between "exit" and "voice" is complicated by the interplay of loyalty, which can affect the cost-benefit analysis whether to pursue a strategy of "exit" or "voice." For example, people may feel a sense of patriotism towards their home country or have brand loyalty towards a product. The presence of loyalty tends

to reduce "exit." "Voice" also increases with the degree of loyalty. As Hirschman states, "a member with a considerable attachment to a product or organization will often search for ways to make himself influential, especially when the organization moves in what he believes is the wrong direction; conversely, a member who wields (or thinks he wields) considerable power in an organization and is therefore convinced that he can get it 'back on track' is likely to develop a strong affection for the organization in which he is powerful."

Loyalty also plays a role in the use of the term 'cyberspace'. Everyone who engages with the term (i.e. those whose "voices" are heard) invests social and political capital in its continued use. This is as true for academics, for whom the success of their book depends on the traction of its concepts, as it is for states, whose power in international negotiations relies on their ability to first frame the issue favorably.

The many path dependencies which manifest as loyalty towards the term 'cyberspace' split those who think about these questions still further. On one hand, despite the many problems identified above, the loyal group feels that–if they work hard enough–they can always change the meaning of the concept for the better. On the other hand, those who "exited" early in favor of other terms have diminishing involvement in the cyber "community," and so translation between the two groups becomes ever more difficult.

DISCUSSION

The purpose of this report was to gain a better understanding of the contests underlying the inconsistent application of the prefix 'cyber'. As the prefix is rarely used alone, we looked at concept 'cyberspace', revealing various forms of contestation. This however leaves us with a question: what does this mean for the recent governance initiatives related to cyberspace?

At minimum, it complicates cyber governance efforts–particularly if policymakers do not recognize the deep-rooted and multi-faceted nature of contestation. Given that neither scholars nor policymakers can come to a general consensus on new 'rules of the road' for cyberspace, an alternative strategy is twofold.

First, all sides should downscale grand initiatives focusing on 'global' solutions for 'everyone' to a variety of more regional and limited agendas. Within such agendas, contests over cyberspace will be resolved *not* through definitional agreement, but

through the creation of shared practices despite such contestation. This strategy moves away from competing 'founding myths', such as those around ARPANET, towards the more prosaic aspects of loyalty above. Institutional power, bureaucratic struggles, reputational concerns, and sheer coincidence have been integral in forming the concept of cyberspace, and will be equally pivotal to its future governance.

Second, the analysis here offers a greater appreciation of what is at stake when we use cyber-related concepts, and shows how much political difference can be contained within linguistic similarity. A better understanding of the underlying normative disagreements will enable them to be brought out into the open, rather than hidden under the empty agreements contained in the cyber prefix. The challenge will be to join both these elements together: the shared practices operating elsewhere in smaller venues, and the open airing of conceptual contestation on the broad issues.

Notes

1 Wiener, Norbert, *Cybernetics Or Control and Communication in the Animal and the Machine*, (Cambridge: MIT, 1961); Betz, David and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power*, (Routledge: The International Institute for Strategic Studies, 2011).

2 Smith, Patrick, "Interview with William Gibson." *The A.V. Club* (September 7, 2010). http://www.avclub.com/article/william-gibson-44836.

3 Ibid.

4 Google Trends, 2016. https://www.google.com/trends/explore#q=cyber%2C%20democracy%2C%20terrorist%2C%20norm&cmpt=q&tz=Etc%2FGMT-2.

5 Ibid.

6 Hayden, Michael, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly*, 5(1) (2011): 3-7, p.3.

7 Walt, Stephen M, "Is the Cyber Threat Overblown?,." *Foreign Policy* (March 30, 2010). http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.

8 Lucas Kello, 'The Meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* 38, no. 2 (1 October 2013): 7–40; Lucas Kello, *The Virtual Weapon and International Order*, (New Haven, CT: Yale University Press, 2017).

9 Nye Jr., Joseph. "International Norms in Cyberspace," *Project Syndicate* (May 2015). http://www.projectsyndicate.org/commentary/international-norms-cyberspace-by-joseph-s--nye-2015-05.

10 Bildt, Carl. "What is the future of cyber governance?" World Economic Forum (2015). https://www.weforum.org/agenda/2015/10/what-is-the-future-of-cyber-governance; Choucri, Nazli, Stuart Madnick and Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," Information Technology for development, 20(2) (2014): 96 -121.

11 Aufderheide, Patricia, *Communications Policy and the Public Interest: The Telecommunications Act of 1996*, (New York: Guildford Press, 1999), p.242.

12 Bremmer, Ian, "Democracy in Cyberspace: What Information Technology Can and Cannot Do," *Foreign Affairs*, (October 21 2010). https://www.foreignaffairs.com/articles/2010-10-21/democracy-cyberspace.

13 Dean, David, Sebastian Digrande, Dominic Field, Andreas Lundmark, James O'Day, John Pineda, and Paul Zwillenberg, "The Internet Economy in the G-20," The Boston Consulting Group (2012). https://www.bcg.com/documents/file100409.pdf; Daugherty, Paul. Prit Banerjee, Walid Negm, and Allan E. Alter, "Industrial Internet of Things: Reimagine the possibilities," Accenture (2015). https://www.accenture.com/us-en/labs-insight-industrial-internet-of-things.aspx; Hurtaud, Stephane, "Cyber Security: Time for a new paradigm," Deloitte (2015), http://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-cyber-security.pdf.

14 Deibert, Ronald, The Growing Dark Side of Cyberspace (...and What To Do About It)," *Penn State Journal of Law & International Affairs*, 1(2) (2012): 260-274

15 Bendrath, Ralph, "The American Cyber-Angst and the Real World – Any Link?" in Robert Latham, ed., *Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security*, (New York: The New Press, 2003); Dunn Cavelty, Myriam, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, (Abingdon: Routledge, 2008); Hansen, Lene, and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly* 53: (2009) 1155–1175; Zajko, Mike, "Canada's cyber-security and the changing threat landscape," *Critical Studies on Security*, 3(2) (2015) 147-161.

16 Brookings Institution, "Cyber" (2016), https://www.brookings.edu.

17 Rid, Thomas and Rob Lee, "OMG Cyber!," *The RUSI Journal*, 159(5) (2008):4-12

18 Ibid.

19 Kello, "The Meaning of the Cyber Revolution," p. 17

20 Libicki, Martin, *Conquest in Cyberspace: National Security and Information Warfare*, (Cambridge: Cambridge University Press, 2007), p.12.

21 Johnson, David R. and David Post, "Law and Borders: The Rise of Law in Cyberspace," *First Monday*, 1 (1-6) (1996).

22 Rid, Thomas and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, 38(1-2): 4-37.

23 Lal, Brij V, *Intersections: History, Memory, Discipline*, (Asia Pacific Publications: Fiji Institute of Applied Studies & Sydney, 2013), p.281.

24 Barlow, John Perry, "A Declaration of the Independence of Cyberspace," Electronic Frontier Foundation (1996), https://www.eff.org/cyberspace-independence.

25 Hurwitz, Roger, "Who Needs Politics? Who Needs People? The Ironies of Democracy in Cyberspace," *Contemporary Sociology*, 28-6: (1999) 655-661, p.656.

26 Barry M., Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, and Stephen Wolff, "A Brief History of the Internet," *ACM SIGCOMM Computer Communication Review*, 39 (5) (2009) 22-31.

27 Cohen-Almagor, Raphael, *Confronting the Internet's Dark Side: Moral and Social Responsibility on the Free Highway*, (Cambridge: Cambridge University Press, 2015), p.67.

28 Nye Jr. Joseph, "Nuclear Lessons for Cyber Security," *Strategic Studies Quarterly*, 5(4) (2015): 18-38, p.24.

29 Hirschman, Albert O., *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*, (Cambridge, MA: Harvard University Press, 1970).

30 Freeman, Julie and Sharna, "Quirke Understanding E-Democracy," *eJournal of eDemocracy and Open Government*, 5(2) (2013) 141-154.

31 Maxey, Levi, "Can Law Restrain Nations in

Cyberspace?," *The Cipher Brief*, (August 6 2017), https://www.thecipherbrief.com/can-law-restrain-nations-cyberspace-1092.

32 Giles, Keir, and William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in K. Podins, J. Stinissen, M. Maybaum, ed., *5th International Conference on Cyber Conflict* (NATO CCD COE Publications, 2013), https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf.

33 Shires, J. (2018). Cybersecurity Governance in the GCC. In R. Ellis & V. Mohan (Eds.), *Rewired: Cybersecurity Governance*. Wiley-Blackwell. Forthcoming.

34 Hirschman, *Exit, Voice, and Loyalty*, p.77-78.

35 Ibid.