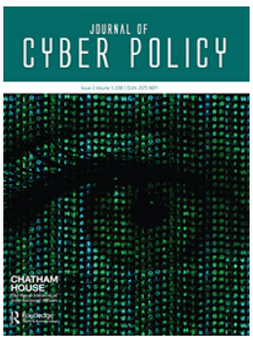

Journal of Cyber Policy

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

Linking cyber strategy with grand strategy: the case of the United States

Valentin Weber

To cite this article: Valentin Weber (2018) Linking cyber strategy with grand strategy: the case of the United States, Journal of Cyber Policy, 3:2, 236-257, DOI: 10.1080/23738871.2018.1511741

To link to this article: https://doi.org/10.1080/23738871.2018.1511741

Published online: 17 Aug 2018.

JOURNAL OF CYBER POLICY
2018, VOL. 3, NO. 2, 236–257
https://doi.org/10.1080/23738871.2018.1511741

Routledge
Taylor & Francis Group

Linking cyber strategy with grand strategy: the case of the United States

Valentin Weber

Department of Politics and International Relations (DPIR), University of Oxford, Oxford, UK

ABSTRACT

The aim of this article is to study whether U.S. cyber strategy is integrated into U.S. grand strategy. In consideration of cyber strategy documents, three case studies and elite interviews find that a link between the two strategic layers is largely missing. Even though U.S. cyber strategy documents contain higher political goals, they do not meet other criteria that indicate links to a grand strategy. Those are a unified list of geopolitical challenges, a balance of ends and means, the integration of military, economic and political means, and the provision of a strategic narrative. Thereby, the documents leave the articulation of grand strategy at the initial stages and do not develop it further. The lack of grand strategy in cyberspace is also visible in U.S. tactical behaviour. The three chosen case studies show that the various U.S. military, economic and political actions taking place under the Obama administration were isolated from each other. Hence, they failed to create a combined impact greater than the sum of their separate effects. This study fills the demonstrated gap in U.S. strategy and concludes by presenting a cyber strategy that is integrated into U.S. grand strategy.

ARTICLE HISTORY
Received 23 January 2018
Revised 6 July 2018
Accepted 11 July 2018

KEYWORDS
Cybersecurity; cyberspace; grand strategy; Stuxnet; United States of America

Introduction

The purpose of this article is to examine whether a grand strategy is visible in the cyber strategy of the U.S. Before proceeding to answer this question, one needs to define the terms 'strategy' and 'grand strategy', as well as illustrate how the former fits into the latter.

Historically, strategy has been a military term comprising a balance between ends and means. Edward Mead Earle (1961) defines it along those lines and claims that strategy is to plan for war and design how to execute war. In 1989, Colonel Arthur Lykke (1989) added 'ways' (course of action) to the 'ends' and 'means' equation. This article uses classical definitions of strategy that see strategy as the balance between ends and means, while omitting 'ways'. Echoing Paul D. Miller (2016), 'ways' are seen as a confusing and incoherent addition to the concept of strategy.

More recently, the term 'strategy' has been extended to the economic (Shatz 2016) and political (Herrmann 1991) realms. Scholars speak of these strategies with regards to the maximisation of power in each field of state contest. Cyber strategy applies to all

CONTACT Valentin Weber valentin.weber@cybersecurity.ox.ac.uk

domains of state contest and is not limited to the military domain, since cyberspace encompasses all realms.

Grand strategy is the highest type of strategy. The use of this term implies that the above-mentioned 'strategic' elements are crucial parts of it. However, in a grand strategy, the ends go beyond military victory. Furthermore, it distinguishes itself from 'policy' by being a plan to achieve policy goals. Policy, in turn, determines the goals (Gray 2010).

While there are many (competing) definitions and approaches to grand strategy,[1] this article operationalises grand strategy as:

- *grand plans* that are a deliberate effort of individuals; mostly found in documents;[2]
- *grand principles*, which are overarching ideas articulated in single words or phrases; the strategy of containment is an illustrative example thereof;
- *grand behaviour*, a 'long-term pattern in a state's distribution and employment of its military, diplomatic and economic resources toward ends' (Silove 2018, 23).

The article proceeds in five sections. The first section reviews the notion of grand strategy, which provides a framework of analysis in five parts for the study of U.S. cyber strategy documents discussed later:

- geopolitical challenges,
- ends,
- a balance of the ends and means,
- the integration of all means of state power,
- strategic narrative; an extension of *grand principles* (e.g. containment) into a strategic story.

In section two, key U.S. policy documents are examined through qualitative content analysis. Sociologist Earl Babbie defines qualitative content analysis as 'the study of recorded human communications' (Babbie 2001, 304). It can involve any communication including written documents, interviews, videos and audio recordings. The procedure of analysis is outlined as the following. A researcher starts to produce summaries of the documents, followed by an explanation of the summaries. Finally, the researcher categorises the material into a clear structure (Mayring 2002). The third section analyses three case studies of U.S. tactical behaviour, which show that each one of them is an isolated action and incoherently integrated with the other tactical behaviours. The case studies examined are Stuxnet (military); an enabling domestic economic environment and open-market policies abroad under President Obama (economic); and U.S. policies on internet governance and freedom under the Obama administration (political). The examined strategy documents and case study analysis are complemented with insights from elite interviews.[3] Semi-structured in-person interviews, lasting approximately an hour were held in Oxford and London, in May and June 2017. The topics covered were pronounced versus unpronounced strategy, integration between U.S. cyber and grand strategy, the IANA (Internet Assigned Numbers Authority) transition, Stuxnet, the Snowden revelations, public–private partnerships between the government and U.S. technology companies, and strategy changes between the Obama and Trump administrations. Participants were chosen due to their cyber-related experience within the U.S. government and

intelligence apparatus, as well as because of their expertise in strategy. The fourth section discusses the findings from section three (strategy documents) and four (tactical behaviour). The fifth section further emphasises the previous results that showcase a lack of connection between U.S. cyber strategy and grand strategy. It fills the void by suggesting a cyber strategy which is consistent with overall U.S. grand strategy.

Theoretical groundings of grand strategy

Grand strategy is important for the study of cyber policy, because it can provide a framework for the study of how prevailing cyber strategy fits into (or contradicts) U.S. grand strategy – assuming it exists.

As illustrated in the introductory lines, there are five major factors that shape grand strategy.

The first factor that forms a grand strategy is the geopolitical challenges that a leader faces. At the most fundamental level, the challenge is to survive in an anarchic world. Mearsheimer (2001), a neorealist scholar of International Relations, for example, maintains that the only way for a state to be secure is to accumulate as much power as possible and thereby increase its power relative to its competitors.

After having articulated the geopolitical challenges, the next step is to define the ends and the means of a grand strategy. The interplay between those two elements defines a country's grand strategy (Trubowitz 2011). Deriving from the different ambition-cost combinations, four broad options arise:

- costly status quo strategy,
- cheap status quo strategy,
- costly revisionist strategy, and
- cheap revisionist strategy.

A status quo strategy translates into keeping power, whereas a revisionist strategy means pursuing an increase in power (Morgenthau 1954). A costly strategy relies mostly on a state's own powers (internal balancing, pre-emptive war) to preserve/change a status quo and is therefore resource-intensive. On the flip side, a cheap strategy is less expensive, because it relies on the sharing of burdens (alliances, buck-passing) to preserve/change the state of affairs.

Grand strategy does, by definition, entail the use of all means available to a state, even though sometimes the threat of using certain means suffices to achieve one's aims. An effective grand strategy integrates the primary means effectively: military, economic and political.

Every comprehensive grand strategy demands a narrative that describes the countries' ends and the means to achieve them. It needs a story with a starting point, an account, and a conclusion that captures the imagination of the domestic population, allies and adversaries (Gray 2015). During the Cold War, the U.S. president was seen as the 'leader of the free world', who would contain the Soviet Union and build a thriving economy with which its society could prosper. But this view has largely disappeared from popular perception. In 1947, it was George F. Kennan's *X Article* that formulated the narrative and guided U.S. policy during the Cold War.

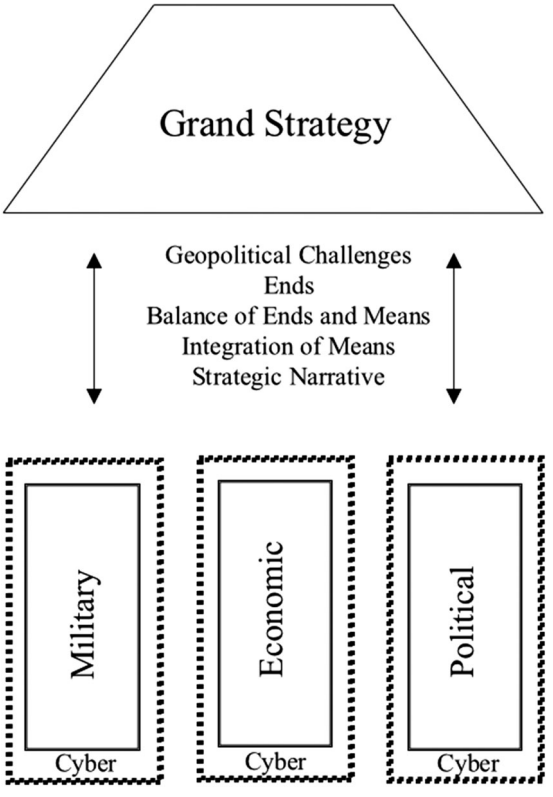

Figure 1. The grand strategic elements in cyberspace are geopolitical challenges, ends, balance of ends and means, integration of means and strategic narrative.

Containment was lauded as an effective grand strategy and described as one of the principal reasons why the U.S. won the Cold War (Gaddis 2013). It was so successful because, on the one hand, it provided a consistent guide for action, spanning four decades and eight presidents, and on the other hand it allowed for flexibility. 'Eisenhower emphasized the limits imposed by economic costs on national security policy, Kennedy expanded the range of strategic tools available to respond to Soviet expansion, and Nixon moved to exploit the Sino-Soviet split' (Martel 2015, 345). Every president had a different approach to implementing grand strategy, but all of them shared a common strategic view.

In 2011, Captain Wayne Porter and Colonel Mark Mykleby attempted to provide a narrative for the twenty-first century. In their article, *A National Strategic Narrative* (Mr. Y 2011) they argue for an open international system and the switch from a zero-sum to a positive-sum view of global politics (Figure 1).

U.S. cyber strategies 2010–2016

Having laid out the theoretical framework of a grand strategy, this study will now move forward and examine selected U.S. cyber strategy documents that were drafted during the Obama administration (Table 1). This article examines six U.S. cyber strategies:

Table 1. Grand strategic elements are spread across different documents.

	Geopolitical challenges	Ends	Balance of ends and means	Integration of means	Strategic narrative
NSS (2010)	Not specified	A cyberspace with continued access, and free flow of information	No	No	No
White House International Strategy for Cyberspace (2011)	Not specified	Open, interoperable, secure, and reliable internet	No	No	Partly
DoD Strategy for Operating in Cyberspace (2011)	Not specified	Open, interoperable, secure, and reliable internet	Yes	No	No
DoD Cyber Strategy (2015)	China Russia North Korea Iran ISIL	Open, interoperable, secure, and reliable internet	Yes	No	No
NSS (2015)	China	Open, interoperable, secure, and reliable internet	No	No	No
DoS International Cyberspace Policy Strategy (2016)	China Russia North Korea Iran	Open, interoperable, secure, and reliable internet	Yes	Yes	Partly

Note: No single strategy unifies all components necessary to make it a holistic strategy integrated with grand strategy.

- The 2011 White House International Strategy for Cyberspace (Obama 2011);
- The 2015 U.S. Department of Defense Cyber Strategy (US Department of Defense 2015);
- The 2016 Department of State International Cyberspace Policy Strategy (US Department of State 2016);
- The 2010 National Security Strategy (Obama 2010);
- The 2011 Department of Defense Strategy for Operating in Cyberspace (US Department of Defense 2011); and
- The 2015 National Security Strategy (Obama 2015).

As an in-depth discussion of the six documents is beyond the scope of this article, it only analyses the first three listed strategies in detail to illustrate the arguments. Synthesised findings of all six documents can be found in Table 1. The chosen documents are the foundation of U.S. cyber strategy, as the selected institutions have been the primary sources of the U.S.'s military, economic and political strategies for decades. Consequently, they are also the most likely candidates for identifying elements of grand strategy in cyberspace.

The analysis of U.S. cyber strategies is divided into five categories that provide a theoretical framework for the analysis: geopolitical challenges, ends, balance of ends and means, integration of means and strategic narrative.

The results of this section are the following. The U.S. has several strategies that lay out a common goal it wants to reach in cyberspace. None of the documents, however, provides all the five elements that would define a comprehensive cyber strategy. Instead, they are scattered amongst the different documents. In essence, the current U.S. strategies are a sum of their constituent parts. They have a value in themselves but do not create

synergies. This points towards an absence of grand strategy in cyberspace, since the defining characteristic of a grand strategy is that it needs to be greater than the sum of its parts.

Geopolitical challenges

2011 White House International Strategy for Cyberspace

The *White House Strategy* does not specify the geopolitical challenges of its time. It enumerates that 'natural disasters, accidents, or sabotage, can disrupt cables, servers and wireless networks on US soil and beyond'. Human challenges are defined as criminal challenges. The U.S.'s major competitors (China, Russia, Iran, North Korea) are not mentioned in the document.

2015 Department of Defense Cyber Strategy

The DoD document refers to four cyberthreat actors:

- China is mentioned the most often (10 times). Problems associated with the Chinese challenge centre on its theft of U.S. intellectual property (IP).
- Russia is mentioned four times. It is considered a serious threat, since

  'Russian actors are stealthy in their cyber tradecraft and their intentions are sometimes difficult to discern' (9).

- Iran (mentioned once) and North Korea (mentioned five times) are described as having developed weaker cyber capabilities, although showing overt hostilities towards the U.S.
- ISIL is listed as the only non-state actor that poses a key cyberthreat.

2016 Department of State International Cyberspace Policy Strategy

The document focuses mostly on China and Russia, being the 'most assertive states advancing alternative visions for international stability in cyberspace and seeking to sway undecided states in regional and multilateral venues' (18). North Korea and Iran are only referred to on the sidelines.

Ends

2011 White House International Strategy for Cyberspace

The document lists one overarching policy priority: an 'open, interoperable, secure, and reliable information and communications infrastructure'. In contrast, it opposes a Balkanization of the internet into national intranets. Even though only few countries have yet attempted to create an internet entirely disconnected from the rest of the world (Sepulveda 2014), certain initiatives have started to fragment the internet. Among those is the adoption of various regulatory regimes across countries and the push for data localisation – the requirement that information is stored in the country that the service is provided in (West and Bleiberg 2014).

2015 Department of Defense Cyber Strategy

The strategy identifies five areas (strategic goals) that the U.S. needs to pursue in order to stay ahead:

- build and maintain ready forces and capabilities;
- defend DoD network, secure data, mitigate risks to DoD missions;
- defend the U.S. homeland;
- build cyber options to control escalation and shape conflict; and
- build and maintain alliances and partnerships.

On top of these five goals is the DoD's commitment to an open, secure, interoperable and reliable internet.

Department of State International Cyberspace Policy Strategy (2016)

The *DoS (Department of State) International Cyberspace Policy Strategy* was broadly inspired by the *2011 White House International Strategy for Cyberspace*. Hence, the policy priority of the two documents is the same: that is to 'work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure' (White House International Strategy for Cyberspace 2011: 8).

Balance of ends and means

2011 White House International Strategy for Cyberspace

The strategy misbalances the ends and means, as it puts too much emphasis on the ends without providing specific means to reach them. For example, it broadly mentions the use of diplomatic means to achieve the goal of an open, interoperable and secure internet. But it fails to describe precisely how this would translate into tangible actions.

2015 Department of Defense Cyber Strategy

The DoD document is clearer on how to achieve its strategic goals than the *2011 White House Strategy*:

(1) To build and maintain ready forces and capabilities, it suggests a viable career path and drawing on the National Guard among others.
(2) To defend the DoD network, secure data and mitigate risks to DoD missions, it proposes assessing the DoD's cyber defence forces and mitigating the risk of insider threats.
(3) To defend the U.S. homeland, it suggests the development of automated information-sharing tools and the assessment of the DoD's cyber deterrence posture and strategy among other things.
(4) To build cyber options to control escalation and shape conflict, it suggests integrating cyber options into combatant command–planning.
(5) To build and maintain alliances and partnerships, it plans to enhance capacities in key regions and counter the proliferation of malware.

2016 Department of State International Cyberspace Policy Strategy

While the policy priorities are the same as in the *2011 White House Strategy*, the means to achieve the goals detailed in the *2016 DoS Strategy* are more specific.

On the military front, the strategy reiterates the need for deterrence by denial and punishment (20). Furthermore, it sees international law as a tool to make the U.S. securer if the military were to be deployed. Specifically, international law could tame potential cyber conflicts by leading states to accept that international law is applicable during conflict.

In economic terms, the document calls for the combatting of market access barriers that hamper the import of U.S. information and communication technology (2). It furthermore suggests contesting data localisation initiatives, as well as imposing economic sanctions if deemed necessary.

To spread its vision of internet governance and internet freedom, the document suggests a continued push for a multistakeholder approach to internet governance, as well as the support of the Internet Governance Forum (IGF). Moreover, it mentions the backing of UN Human Rights Council Resolutions on online rights as a means to reach its goal. In the technical realm, it argues for the continuation of financial support for secure communications technology and anti-censorship tools.

Integration of means

2011 White House International Strategy for Cyberspace

The strategy encourages the U.S. to use all means of state power. However, it omits the integration between them.

On the military frontlines, the U.S. will rely on deterrence by denial and punishment to protect its networks (13–14).

In economic terms, the U.S. will foster a free-trade environment and work to protect intellectual property from theft (17). While this goal is clearly stated, concrete measures to implement it are not provided.

In the political realm, the U.S. will work to ensure the security of the domain name system and the internet's underlying infrastructure. Furthermore, it will support a multistakeholder internet governance approach and will continue to endorse the Internet Governance Forum as a venue of internet governance discussion. In addition to this, it will collaborate with civil society to increase its cyber security.

2015 Department of Defense Cyber Strategy

The *DoD Cyber Strategy* does not integrate the military means with all other means that are available to the government. It does specify cooperation between the FBI and the DHS, but it remains vague on collaboration with other government departments.

2016 Department of State International Cyberspace Policy Strategy

The strategy champions the use of all tools available (a whole-of-government approach) to reach the goals set out. It names collaborations with a wide range of government departments such as the Department of Homeland Security, the Department of Commerce and the National Institute of Standards and Technology. It also recognises the need for diplomatic, law enforcement, economic, military and intelligence capabilities with regard to deterrence.

Strategic narrative

2011 White House International Strategy for Cyberspace

The document attempts to provide a strategic narrative. It shows the U.S. vision of the internet and juxtaposes it with the alternative internet vision of Russia and China, which emphasises a fragmented cyberspace of sovereign nations. However, the strategy does not provide a full narrative, because it does not recognise the importance of cyberspace for the overall geostrategic chessboard. It does not create a link to a larger strategy.

2015 Department of Defense Cyber Strategy

No comprehensive strategic narrative can be identified in the document.

2016 Department of State International Cyberspace Policy Strategy

The document hails the U.S. multistakeholder vision of the U.S. but reviews the Chinese and Russian alternatives to the U.S. vision in technical and descriptive, rather than engaging language. Similarly to the *2011 White House Strategy*, it does not place cyberspace into a larger context of the geostrategic game.

U.S. behaviour in cyberspace

The following section will examine U.S. tactical behaviour and its strategic effects on the military, economic and political realms of cyberspace. Before delving into the empirics, it is necessary to clarify what one means by tactics, strategy and strategic effect. 'Tactics is all about action, doing things, while strategy is about the consequences of the preceding tactical behaviour' (Gray 2015, 3). Strategic effect, in turn, can only be in the consequences of what we do.

This distinction is important, as it highlights that actions can never be strategic, only the results can be. The primary focus of this section is precisely this strategic effect/result, which can be measured in two ways. Firstly, Colin S. Gray (2010) claims that 'the strategic effect of primary interest is manifested in the perceptions, judgements, and behavioural choices of a human enemy'. Secondly, strategic effects can be measured by observing tactical behaviour that gives the executing nation a strategic advantage or disadvantage. Research and investment, for instance, bring about a strong technology sector that in turn provides advanced technology for warfare or other state purposes.

The ensuing section shows that U.S. tactical behaviour produced positive strategic effects in different fields of state activity. However, I argue that the U.S. could have achieved much greater impact and produced a whole that is larger than the sum of its parts if it had integrated its behaviour in the military, economic and political fields.

U.S. military behaviour in cyberspace

The first example of tactical behaviour with strategic impacts analysed in this article transpired in the military domain.[4] In 2010, Belarusian security researchers discovered the computer worm Stuxnet (Zetter 2014). Stuxnet was intended to sabotage centrifuges in Natanz, an Iranian nuclear facility – and it did so successfully by damaging the centrifuge rotors, which are central to the uranium enrichment process (Langner 2013). However, the

worm, which was initially delivered via a USB stick, started to spread uncontrollably and infected thousands of computers worldwide (Markoff 2010). This is how the Belarusian security researcher discovered the virus on one of their client's computers.

It soon became widely accepted that the United States and Israel were behind the malware that infected systems in order to delay Iran's suspected nuclear weapons programme (Gates 2012). The attack became known as the first major deployment of a physically destructive cyberattack outside of supervised experiments (Langner 2013).

Stuxnet had several strategic impacts:

- It set new norms for state behaviour in cyberspace.
- It spurred competitors in their respective spending on cyber capabilities.
- It impacted the Iranian nuclear talks.

First, the deployment of Stuxnet, formally dubbed Operation Olympic Games, is described as being similar to the use of Zeppelin airships during WWI. Arquilla (2015) makes an analogy and explains that just as the Zeppelins were the first rudimentary weapons of air power, Stuxnet might mean the dawn of cyberweapons. Adam Segal (2016) names 2012 – the year Stuxnet was leaked publicly – as 'Year 0. General Michael V. Hayden describes the attacks on Iran by saying 'someone crossed the Rubicon', referencing Caesar's river crossing from which there was no point of return. Michael V. Hayden continues by asserting 'we've got a legion on the other side of the river now. I don't want to pretend it's the same effect, but in one sense at least, it's August 1945' (Sanger 2012b). While an allusion to August 1945 and the dropping of nuclear bombs may be a bit far-fetched, Stuxnet has been a norm-setter in cyberspace. It might have also signalled to its competitors that the U.S. is not in demise. In contrast, the analogy to 1945 serves to showcase that the U.S. is again in 1945, when it started to define the twentieth century as the American century. Likewise, the twenty-first century might become the second American century.

Second, the norm-setting impact might have influenced U.S. competitors to pay more attention to their own cyber capabilities. This leads to a second potential strategic impact of Stuxnet: increased spending on cyber capabilities. In recent years China's spending on cyber capabilities saw a 20–30% increase compared to previous years (Gertz 2015). While China might have increased spending regardless of other actors, Stuxnet may have encouraged China to devote more funds to cyber capabilities. Strategically this means that the closing gap in spending between U.S. and China may also translate into a decreasing gap in capabilities.

The third strategic effect of Stuxnet is that it weakened the Iranian negotiating position during the nuclear talks. Stuxnet specifically impacted the cost-benefit calculation of constructing a nuclear weapon. In the words of General Michael V. Hayden:

> Ideally, if someone was going to do that [Stuxnet] they would try to do it in a way where the hand is hidden and that the Iranians believed they did not know how to do this. Now, once it becomes public and the Iranians think they know who did it, you know there is still another good effect. How far are the Americans willing to go? That made the negotiations a little more attractive to the Americans.[5]

In addition to having a deterrence effect, Stuxnet also led Iran to doubt its ability to construct a functioning nuclear weapon. This meant that economic sanctions and other costs associated with building a weapon of mass destruction became more painful. Why would one bear the costs of constructing a nuclear bomb if one was not technically able to reach this goal? Since Iran believed that it may be unable to build a nuclear bomb, the nuclear programme could now be used as a bargaining chip during negotiations. A halt of the programme was in sight. This view is further underpinned by a partaker in the attack, who claimed that 'the intent (of Stuxnet) was that the failures should make them feel they were stupid, which is what happened'. 'They overreacted', a U.S. official said. 'We soon discovered they fired people' (Sanger 2012a).

U.S. economic behaviour in cyberspace

The second U.S. tactical behaviour with strategic effects concerns the economic domain and is materialised in an enabling environment at home coupled with an open-market policy abroad. The combination of those two policies resulted in major technology companies being established.

First, providing an enabling economic environment. The U.S. government has been crucial in the creation of the internet through the military's ARPANET (Advanced Research Projects Agency Network). This inception has brought it until today a strong control over the global internet infrastructure and a first-mover advantage when it comes to internet standards and regulations. U.S. policymakers soon perceived the internet not only as a unique source of U.S. military strength but also of economic power and have therefore argued for its privatisation in a low-regulatory manner that would encourage risk-taking. 'The Atari Democrats', a group within U.S. Congress, was crucial in launching the Clinton-Gore wave of privatisation of the internet in the mid-1990s, which was intended to extend the internet from the military to the economic sector and hence link it to U.S. economic power (Carr 2016).

The government-led research and development agenda in a low-regulatory environment has continued since then in the form of extensive funding. The U.S. has always invested in companies that might become innovators domestically. Google founders Sergey Brin and Larry Page, for example, initiated the first website-ranking application with funding from the Digital Library Initiative, a joint undertaking of the NSF (National Science Foundation), DARPA (Defense Advanced Research Projects Agency), and NASA (National Aeronautics and Space Administration) (NSF 2004). Similarly, Apple received early state investments from the U.S. Small Business Investment programme. Only after government funding showed results did Apple attract further investments from venture capitalists (Mazzucato 2013). Government funding continues into the present with a plethora of technology start-ups benefitting from In-Q-Tel (a venture capital arm of the CIA) and DARPA investments (Crunchbase 2018a, 2018b).

Second, the United States has pushed abroad for open markets and a free-trade environment, which allowed GAFA-like companies (Google, Apple, Facebook and Amazon) to spread (Obama 2011, 17). During the WCIT (World Conference on International Communications) negotiations, for example, the U.S. argued that the internet ought to: 'require no global regulatory regime and that all these systems will thrive wherever there is free and open access to content and information' (US Department of State

2012). During the negotiations, U.S. officials worked together with the private sector in order to make those propositions more forceful. Fittingly, Google published a website warning that censorship and regulation may encroach on information freedom, ahead of the conference (Jablonski and Powers 2015, 120).

U.S. officials also initiated the TPP (Trans-Pacific Partnership), which would have reduced tariffs on exports of information and communications technology products and liberalised trade in software and internet-provider services (Council on Foreign Relations 2015).

In other words, both during the WCIT and TPP negotiations Washington promoted a liberal and deregulated internet, where U.S. companies could export technology and information, and set U.S. standards without any trade barriers or inhibitions from national regulators across the world.

Research and development

The first strategic effect that major U.S. technology companies have on U.S. power is that they create an information asymmetry between the U.S. and other countries. A lot of valuable data travels through the U.S., because major telecommunications and service providers have their headquarters in the U.S. To be more specific, 70% of world internet traffic passes through Loudon County, Virginia alone (Loudon Virginia n.d.). The NSA has real-time access to this data, having installed surveillance equipment in Internet Exchange Points (IXPs) across the United States – IXPs are key choke points of the internet infrastructure (Deibert 2013). Bruce Schneier (2014) coined the term 'public-private surveillance partnership', meaning that the public–private partnership goes beyond cooperation on technology transfer.

The second strategic impact of having large technology companies is that they give the U.S. an innovative edge. Breakthroughs in technology happen increasingly in the private sector and not via government-funded programmes. This is due to two factors: U.S. technology companies have grown considerably since the Clinton-Gore wave of privatisation and have accumulated large budgets for research and development. Furthermore, private technology firms have access to great amounts of data, as well as analytical capabilities, and are therefore in a better position to develop more powerful algorithms than governments. Moreover, they are not as bound by restrictions as government agencies are, since users give private companies their consent through the terms and conditions. Consequently, companies can use this valuable data for research and development.

Open-market policy

The third strategic impact that U.S. technology companies bring to their government springs from the open-market policy that the U.S. has pursued. This allows companies to diffuse internationally, consequently setting worldwide technology standards. Secure communications and the easy dissemination of information for individuals are typically built into Apple, Google or Microsoft programs and devices. Those in-built characteristics are in the interest of the U.S., as they fulfil the U.S.'s vision of the free flow of information. In other words, technical devices advance an 'open, interoperable secure and reliable cyberspace' (Obama 2011, 3). This is because internet protocols, standards and platforms are political by design, and they 'shape social and economic structures ranging from individual civil liberties to global innovation policy' (DeNardis 2014, 7). Professor Joseph Nye Jr. gives

another example of how setting standards in the technology sector can be a kind of soft power and hence be in the U.S.'s strategic advantage:

> information instruments can be used to produce soft power in cyberspace through agenda-framing, attraction or persuasion. For example, attracting the open source software community of programmers to adhere to a new standard is an example of soft power targeted within cyberspace. (2011: 175)

U.S. political behaviour in cyberspace

The third U.S. tactical behaviour considered in this study is visible in the political domain and is cemented in two policies. First, the U.S. promotes a multistakeholder approach to internet governance. Second, the U.S. argues for keeping the internet a space where information can flow freely. It has had widespread success with both policies. This is seen in the strategic impacts of each policy.

Multistakeholder approach

The U.S.'s multistakeholder policy on internet governance is perceivable in speeches (Pritzker 2014), national strategy documents (Obama 2011), and international declarations (World Summit on the Information Society 2005). The stakeholders involved are defined (World Summit on the Information Society 2005) as:

- states (policy authority);
- private companies (driver of internet development);
- civil society (shaper at a community-level);
- intergovernmental organisations (facilitator of policy coordination); and
- international organisations (locus of internet-related technical standards and policies).

Although multistakeholderism is presented as an overwhelmingly positive governance model by U.S. leaders, one has to admit that it is not a panacea. Multistakeholder organisations such as ICANN have been notorious for lacking accountability and legitimacy, and for entrenching inequalities through the cementing of U.S. power over internet governance (Raymond and DeNardis 2015). To counter these trends, the multistakeholder process needs to empower a more representative sample of private sector actors and a wider range of civil society actors (Radu, Zingales, and Calandro 2015).

The latter, multilateral model is being hailed by China and Russia. China, in particular, has lobbied many developing countries to sign up to its proposals at international conferences. In 2012, its efforts bore fruits at the International Telecommunications Union's world conference in Dubai. Eighty-nine states, forming a majority, subscribed to the new International Telecommunications Regulations favoured by China and Russia (WCIT 2012).

So far, the strategic effects are difficult to measure, but the U.S. is largely managing to fend off Chinese and Russian resolutions at international conferences that call for a multilateral internet governance model and the giving of more powers to the ITU – with certain exceptions, such as the 2012 ITU conference in Dubai (Inkster 2016). In other words, the U.S. is successful in keeping a large amount of countries subscribing to its vision of internet governance and thereby impacting their behaviour. The U.S. has also long kept power over one of the central internet governance organisations, the Internet Corporation for

Assigned Names and Numbers (ICANN). For years, ICANN's functioning remained under the stewardship of the U.S. Department of Commerce (IANA Stewardship Transition Coordination Group 2016). This gave Washington the ability to 'have exclusive authority over aspects of Internet governance that are critical to all states' (Mueller and Kuerbis 2014, 2). It might seem counter-intuitive that it then transferred oversight of IANA (Internet Assigned Numbers Authority), a function of ICANN, from the U.S. Department of Commerce to ICANN's global multistakeholder community in 2016 (Malcolm 2016).

However, holding onto control would have had negative strategic effects. In the words of General Michael V. Hayden:

> despite a lot of conservative concern in America complaining about this being one more example of Obama giving away American stuff, I actually think this was a smart move. We are sharing control of this with like-minded, like-valued, like-interested nations.[6]

General Hayden continues by saying that by endorsing a multistakeholder approach the U.S. created a third option. Option number one was to keep the current situation of U.S. oversight. Option number two was handing control over to the ITU (International Communications Union), which would have been in the Chinese and Russian interest. According to General Hayden, change in oversight was inevitable. What the U.S. did is to steer it into its strategic advantage. 'We started a fire that was designed to burn the underbrush. So when the big fire comes it can be extinguished'.[7]

This is a strategic effect in political rather than in military or economic terms, and its nature is soft rather than hard. As Professor Joseph Nye Jr. (2011) writes in the *Future of Power:* 'the target's acquiescence in the legitimacy of the agenda is what makes (it) … partly constitutive of soft power – the ability to get what you want by the co-optive means of framing the agenda, persuading, and eliciting positive attraction'.

Internet freedom

The second U.S. policy is the facilitation of the free flow of information. For example, during WWII and the Cold War, it used *Voice of America* to counter enemy propaganda and to disseminate information (McMahon 2009). More recently, the American stance on information freedom was observable in its support to keep Twitter online during the Iranian revolution in 2009 (Musgrove 2009), as well as in Secretary of State Clinton's speeches on 'internet freedom'. Clinton (2010) mentions that the U.S.'s goal is to 'encourage and support increasing openness in China, because we believe it will … further add to … the democratisation on a local level that we see occurring'. The U.S.'s internet freedom agenda seems, however, to have lost traction (MacKinnon 2012). One reason for this is Edward Snowden's disclosure of U.S. spying activities, which caught U.S. strategists by surprise. It also dealt a serious blow to their ability to name and shame other countries' human rights violations. Another reason for a decline of information freedom is that Russia and China are actively exporting their models of internet censorship to other countries, hence strengthening information controls at the expense of freedom (Weber 2017).

Discussion

The following section argues that U.S. grand strategy is absent in U.S. cyber strategy. For a grand strategy to be detected in cyberspace, several criteria need to be met: a unified list

of geopolitical challenges, higher political goals, a balance of ends and means, an integration of military, economic and political means, and an underlying strategic narrative justifying all previous elements. While the higher political goals are defined, the strategy documents, the case studies and the expert interviews all fail to indicate that the other criteria are met.

The articulation of grand strategy is initiated in the various strategy documents but not developed further. With regards to the geopolitical challenges, the different strategies mention different threat actors. There is no common denomination of threats between the documents.

By contrast, the overarching ambition is clear. All examined strategies have one common theme: an open, secure, interoperable and reliable internet that enables the free flow of information.

However, the stated goals lack an underlying strategic narrative. The *2011 White House Strategy* and the *2016 DoS Strategy* are the only examined strategies that have attempted to establish a strategic narrative. They lay out the U.S. vision of the internet and how an alternative model of the internet might look. However, they fail to explain the importance of cyberspace in the overall geostrategic view and how cyberspace can be used to achieve goals beyond the domain. One of the reasons for the missing strategic narrative may be that the *2011 White House Strategy*, despite its name, was intended as a policy statement rather than a strategy document.

While the strategies mention the integration of military, economic and political tools, they do not say why this should be done or how it should be done. They neither state what role each tool plays in the grand strategy nor how the tools can be used concurrently to increase U.S. influence. Furthermore, they fail to explain what the balance is between the ends and means. For all of the above reasons, this article argues that a U.S. grand strategy is unidentifiable in cyberspace.

The findings in the documents are reinforced by U.S. tactical behaviour. The nation's actions in the military, economic and political realms were incoherent and isolated from each other. All three tactical behaviours achieved strategic impacts. However, they did not create or allow for synergy to emerge between them. They failed to produce a combined impact greater than the sum of their separate effects.

While this article focuses on cyber and grand strategy under President Obama, commentators and pundits have made observations on whether the Trump administration has changed or continued past practices. Weitz (2018) argues that the *2017 National Security Strategy* remains a continuation of previous U.S. strategy documents. Michael Sulmeyer's account (2017) of the *NSS's* cyber components largely confirms this viewpoint, in the sense that the strategy mentions similar geopolitical challenges – China, Russia, North Korea, Iran and terrorism. The *NSS*'s goals too remain the same in cyberspace. Those are an open, interoperable and secure internet. However, despite the publication of this latest strategy document, pundits and policymakers alike, including Senator McCain (Levine 2017), Senator Sasse (2018), and David E. Sanger (2018), have been pointing out that the U.S. still lacks a cyber strategy.

Considering all of the above, one may wonder why cyber and grand strategy are not linked with each other. One possible explanation is that the U.S. did not have a grand strategy under President Obama. Hence, it could not link its cyber strategy with its grand strategy. The question of grand strategy under the Obama administration is very much

disputed and out of the scope of this article.[8] In either case, the existence or non-existence of a grand strategy would not affect the argument, which is that the U.S. does not link the two strategic layers.

Meijer and Jensen's (2018) work on contemporary grand strategies provides several alternative explanations for why an interlinkage might not have happened. The authors mention that 'growing volume, velocity, and diversity of interactions within international society – alters states' strategy formation processes' (1). To give an example, the foreign ministries are no longer the sole gatekeepers of foreign affairs. A variety of ministries and private actors compete on matters of foreign affairs, create working groups and links with foreign nations (Lequesne and Weber 2016). Furthermore, states produce an increasing amount of strategies. With regards to cybersecurity, the U.S. Coast Guard, the U.S. Department of Energy, the U.S. Department of State and a plethora of other departmental organisations publish their respective strategies. The sheer amount of strategies further impedes coherence in the crafting and interlinking of cyber and grand strategy. In sum, the above-mentioned factors diminish the capability of states to craft coherent strategies on a horizontal axis (military, economic, political) and interlink the different strategic levels on a vertical axis (strategy, grand strategy).

Policy recommendation

This article has demonstrated that several indicators of U.S. grand strategy – although scattered – are to be found in cyber strategy documents. Nevertheless, U.S. cyber strategy does not go beyond the initial articulation of how it fits into U.S. grand strategy. The following section will propose a cyber strategy that fills this void. It is different from previous strategy documents in three aspects:

- It integrates all elements that create a link between cyber and grand strategy into one document.
- It urges the U.S. government to cooperate with the private sector to advance cyber norms globally and especially with companies in countries undecided about internet governance.
- It contains a blueprint for a comprehensive strategic narrative.

Based on the analysis of strategy above, the major geopolitical challenges are identified as China and Russia, since they are the primary competitors with the United States in the military, economic and political domain. Their revisionist behaviour has caused major concern, e.g. Russian meddling in U.S. elections and Chinese economic espionage.

In essence, this article suggests that strong defensive and offensive cyber capabilities will allow the U.S. not to dominate but to retain primacy in the military domain.

Primacy in the military domain will be underpinned by the continuation and expansion of long-term investments in promising technology companies via government funding, e.g. DARPA and In-Q-Tel. This has been successful in the past (Dembosky 2013) and should be continued in the future. At home, the research and development agenda will allow companies to innovate. Abroad, the U.S. should continue to pursue a policy of open markets that will allow domestic companies to diffuse internationally. The government needs to stay in touch with companies as they mature and share the benefits

through public–private partnerships. In times when innovation is shifting from the public to the private sector, this will allow the U.S. to stay ahead of other competing countries.

While the U.S.'s economic strategy in cyberspace will advance its military edge, the political strategy in cyberspace will reinforce both the military and economic strategies. The U.S. ought to push through diplomatic means for a multistakeholder governance model and facilitate the free flow of information. It should at the same time work on addressing the lack of accountability and legitimacy of multistakeholder institutions to build trust in its vision for internet governance. It should build a community of like-minded nations that it can rely on in its struggle with autocratic countries. The U.S. may also consider supporting norm-building measures in the private sector (Sanger 2018). This would allow the U.S. to multiply forces in its endeavours to build norms in cyberspace with help from the private sector at home and abroad. In this sense the U.S. would continue trying to persuade undecided nations, such as Brazil, India, and South Africa, to support the multistakeholder internet governance model (Maurer and Morgus 2014). In addition to this, it would encourage companies that operate within these nations to follow cyber norms that protect civilians and human rights and reduce the risk of cyber conflict. In contrast to Huawei and ZTE, which are quasi-state companies, and have few incentives to sign up to such a set of norms, companies in undecided nations may be more inclined to subscribe to these ideas and hence build a critical mass of norm adherers. The creation of such a community will foster collaboration of the same community in different fora with foci other than cyberspace.

The military, economic and political actions shall be integrated in this way. The combined effect created shall become greater than the sum of its parts and allow for the common goal of an 'open, interoperable secure and reliable cyberspace to be achieved' (Obama 2011).

An open and interoperable internet is the only way to maintain international security,[9] stability and a way of life-based on freedom and the free flow of information in cyberspace. The alternative to the U.S. model of information freedom shall be juxtaposed with the authoritarian model, which tells the story of Balkanized national intranets that rely on pervasive censorship measures and unchecked domestic surveillance.

The consequences of the realisation of the latter model would be a world where governments have an unquestioned permission to decide what information is good for their citizens and what is not. This would likely incite governments to abuse their powers. For all of these reasons, the former model will prevail over the latter and gain attraction through its positiveness.

As the cyber domain encompasses each realm of state activity, the U.S.'s position in cyberspace will have major repercussions on its overall standing in the international system. The recognition of challenges, definition of goals, the balance between the two, the integration of all means of U.S. power, and most importantly, an effective communication of all the above, will ensure that the synergies created in cyberspace will be reflected in the U.S.'s overall prowess.

To conclude, the above laid out conceptualisation of a grand strategy in cyberspace will allow the U.S. and like-minded nations to retain superiority in the great game of influence in cyberspace and beyond. Many elements are already present – the U.S. only needs to articulate them in a cohesive and clear manner. The development of such a narrative

will supply Washington with something Kennan's *X Article* provided during the Cold War – that is an overarching guide to steer foreign policy decisions.

Notes

1. Silove (2018) provides one of the most complete studies of just what has been defined as grand strategy. She categorises previous literary works into three categories: literature that conceives of grand strategy as a plan that details ambitions (e.g. Feaver 2009; Krasner 2010), an organising principle that guides actions (e.g. Dueck 2015; Brands and Porter 2015), and behaviour (e.g. Luttwak 2009; Narizny 2007). Martel (2015), for his part, categorises approaches to grand strategy into four categories: those of social scientists, historians, military strategists and practitioners. Each of these groups has its own methodologies, social backgrounds and analytical frameworks, which eventually result in different conceptions of grand strategy.
2. Strategies are laid out in military documents, e.g. 2014 Quadrennial Defense Review and the 2015 Department of Defense Cyber Strategy. One may interject that strategies do not necessarily need to be formulated in order to exist (Hemmer 2015, 4). Hemmer implies that grand strategies can be executed unintentionally and be deduced from behaviour – grand behaviour. In addition to this, any proposed strategy gets distorted by policymaker biases during the drafting period and organisations' limitations during its implementation (Betts 2000). This makes a detection thereof more difficult. However, if one conceives of grand strategy as an intentional plan – a grand plan – then it needs to be communicated to a certain degree. The United States is a country with a large bureaucratic structure. If bureaucrats are unaware of what the stated policy is, they will be unable to implement it (interview with Professor Richard J. Harknett). The fundamental question is: would any strategy have force without institutions (interview with James de Waal)? Furthermore, countries pronounce their strategies to signal their intent to allies, competitors and adversaries.
3. Participants and interview dates: James de Waal, 8 May 2017; Professor Christopher Coker, 2 June 2017; Professor Joseph S. Nye Jr., 8 June 2017; Professor Richard J. Harknett, 24 May 2017; General Michael V. Hayden, 9 June 2017.
4. For more political and strategic context see (Farwell and Rohozinski 2011; Gompert and Libicki 2015; Lindsay 2013), for technical analysis consult Byres, Ginter, and Langill (2011), De Falco (2012), and Falliere, Murchu, and Chien 2011).
5. Interview with General Michael V. Hayden.
6. Interview with General Michael V. Hayden.
7. Interview with General Michael V. Hayden.
8. Interviews with Professor Christopher Coker; Professor Joseph S. Nye Jr.; Professor Richard J. Harknett; Michael Hayden.
9. An open and anonymous internet may also weaken security, since it reduces the ability to attribute attacks at the expense of privacy (Carr 2016, 116). However, U.S. policymakers perceive that social power gained from an open network outweighs the relative decrease in security.

> [US] Politicians repeatedly express the view that the most assured route to security (and the preservation of US power) is through continuing to adhere closely to the ideas and values which have been the foundations of US power in the past and that they believe will continue to be in the future … Although they use the language of norms and values, this should not undermine the strategic reasoning behind this choice. (184)

Acknowledgements

I am indebted to Lucas Kello, Joss Wright, Benjamin Jensen, Jantje Silomon, Lennart Maschmeyer and Jamie Collier for their insightful comments on this article. An early version of this article was presented at ISSS-ISAC Annual Convention, Washington, DC (2017).

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

This work was supported by the Engineering and Physical Sciences Research Council UK.

Notes on contributor

Valentin Weber is a D.Phil. Candidate in Cyber Security at the Centre for Doctoral Training in Cyber Security, based at the Department of Politics and International Relations, and a Research Affiliate with the Centre for Technology and Global Affairs, University of Oxford. His current research focuses on cyber strategy as well as the diffusion of cyber norms.

ORCID

Valentin Weber http://orcid.org/0000-0002-6473-990X

References

Arquilla, John. 2015. "Deterrence after Stuxnet." CACM. https://cacm.acm.org/blogs/blog-cacm/190371-deterrence-after-stuxnet/fulltext.

Babbie, Earl R. 2001. *The Practice of Social Research*. Belmont, CA: Wadsworth Thomson Learning.

Betts, Richard K. 2000. "Is Strategy an Illusion?" *International Security* 25 (2): 5–50.

Brands, Hal, and Patrick Porter. 2015. "Why Grand Strategy Still Matters in a World of Chaos." National Interest. http://nationalinterest.org/feature/why-grand-strategy-still-matters-world-chaos-14568.

Carr, Madeline. 2016. *US Power and the Internet in International Relations*. Basingstoke: Palgrave MacMillan.

Clinton, Hillary. 2010. "Secretary Clinton Remarks Internet Freedom." C-SPAN. https://www.c-span.org/video/?291518-1/secretary-clinton-remarks-internet-freedom.

Council on Foreign Relations. 2015. "The Top Five Cyber Policy Developments of 2015: The Trans-Pacific Partnership." Council on Foreign Relations. https://www.cfr.org/blog/top-five-cyber-policy-developments-2015-trans-pacific-partnership.

Crunchbase. 2018a. "In-Q-Tel Investments." Crunchbase. https://www.crunchbase.com/organization/in-q-tel/investments/investments_list#section-investments.

Crunchbase. 2018b. "DARPA." Crunchbase. https://www.crunchbase.com/organization/darpa#section-investments.

De Falco, Marco LTC. 2012. "Stuxnet Facts Report: A Technical and Strategic Analysis." NATO CCDCOE. https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf.

Deibert, Ronald. 2013. *Black Code: Inside the Battle for Cyberspace*. Toronto: Signal.

Dembosky, April. 2013. "Silicon Valley Rooter in Backing from US Military." *Financial Times*. https://www.ft.com/content/8c0152d2-d0f2-11e2-be7b-00144feab7de.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Dueck, Colin. 2015. *The Obama Doctrine: American Grand Strategy Today*. New York, NY: Oxford University Press.

Earle, Edward M. 1961. *Makers of Modern Strategy: Military Thought from Machiavelli to Hitler*. Princeton, NJ: Princeton University Press.

Eric, Byres, Andrew Ginter, and Joel Langill. 2011. "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems." Barr-Thorp Electric Co., Inc. http://www.barr-thorp.com/wp-content/uploads/2011/04/how-stuxnet-spreads.pdf.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2011. "W32.Stuxnet Dossier." Symantec. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
Farwell, James, and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival* 53 (1): 23–40.
Feaver, Peter. 2009. "What Is Grand Strategy and Why Do We Need It?" Foreign Policy Shadow Government. http://foreignpolicy.com/2009/04/08/what-is-grand-strategy-and-why-do-we-need-it/.
Gaddis, John Lewis. 2013. "Cold War, Containment, and Grand Strategy: An Interview with Pulitzer Prize-Winning Historian John Lewis Gaddis." *Yale Journal of International Affairs* 8 (1): 73–77. http://yalejournal.org/wp-content/uploads/2013/03/Gaddis.pdf.
Gates, Guilbert. 2012. "How a Secret Cyberwar Program Worked." *New York Times*. http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html.
Gertz, Bill. 2015. "Cheers to Good Frenemies! China Investing in Cyberwarfare Superiority." *Washington Times*. http://www.washingtontimes.com/news/2015/apr/1/china-invests-cyberwarfare-compete-us-military/.
Gompert, David C., and Martin Libicki. 2015. "Waging Cyber War the American Way." *Survival* 57 (4): 7–28.
Gray, Colin S. 2010. *The Strategy Bridge: Theory for Practice*. Oxford: Oxford University Press.
Gray, Colin S. 2015. *The Future of Strategy*. Cambridge: Polity.
Hemmer, Christopher M. 2015. *American Pendulum: Recurring Debates in U.S. Grand Strategy*. Ithaca, NY: Cornell University Press.
Herrmann, Richard K. 1991. "The Middle East and the New World Order: Rethinking U.S. Political Strategy After the Gulf War." *International Security* 16 (2): 42–75. doi:10.2307/2539060.
IANA Stewardship Transition Coordination Group. 2016. "Proposal to Transition the Stewardship of the Internet Assigned Numbers Authority (IANA) Functions from the U.S. Commerce Department's National Telecommunications and Information Administration (NTIA) to the Global Multistakeholder Community." ICANN. https://www.icann.org/en/system/files/files/iana-stewardship-transition-proposal-10mar16-en.pdf.
Inkster, Nigel. 2016. *China's Cyber Power*. London: Routledge for IISS.
Jablonski, M., and Shawn M. Powers. 2015. *The Real Cyber War: The Political Economy of Internet Freedom*. Urbana: University of Illinois Press.
Krasner, Stephen D. 2010. "An Orienting Principle for Foreign Policy." *Policy Review* 163: 3–12.
Langner, Ralph. 2013. "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve." Langner. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.
Lequesne, Christian, and Valentin Weber. 2016. "L'influence Du Service Européen Pour l'Action Extérieure Sur Les Ministères Des Affaires Étrangères : Une Comparaison France-Autriche." *Revue Française d'Administration Publique* 158 (2): 505–15.
Levine, Mike. 2017. "McCain Threatens to Subpoena Trump's Cybersecurity Czar After He Skips Hacking Hearing." *ABC News*. https://abcnews.go.com/Politics/mccain-threatens-subpoena-trumps-cybersecurity-czar-skips-hacking/story?id=50593296.
Lindsay, Jon R. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404.
Loudon Virginia. n.d. "Business & Industry Stats." Loudon County Economic Development, VA. https://biz.loudoun.gov/information-center/business-industry-stats/.
Luttwak, Edward. 2009. *The Grand Strategy of the Byzantine Empire*. Cambridge, MA: Belknap Press of Harvard University Press.
Lykke, Colonel Arthur F. Jr. 1989. "Defining Military Strategy." *Military Review* 69 (5): 2–9.
MacKinnon, Rebecca. 2012. *Consent of the Networked: The World-Wide Struggle for Internet Freedom*. New York, NY: Basic Books.
Malcolm, Jeremy. 2016. "Oversight Transition Isn't Giving Away the Internet, But Won't Fix ICANN'S Problems." Electronic Frontier Foundation. https://www.eff.org/deeplinks/2016/09/oversight-transition-isnt-giving-away-internet-wont-fix-icanns-problems.
Markoff, John. 2010. "A Silent Attack, But Not a Subtle One." *New York Times*. https://www.nytimes.com/2010/09/27/technology/27virus.html.

Martel, William C. 2015. *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy*. New York, NY: Cambridge University Press.
Maurer, Tim, and Robert Morgus. 2014. "Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate." Centre for International Governance Innovation. https://www.cigionline.org/sites/default/files/no7_2.pdf.
Mayring, Philipp. 2002. *Einführung in die qualitative Sozialforschung*. Weinheim: Beltz.
Mazzucato, Mariana. 2013. "Taxpayers Helped Apple, but Apple Won't Help Them." *Harvard Business Review*. https://hbr.org/2013/03/taxpayers-helped-apple-but-app.
McMahon, Robert. 2009. "Channeling the Cold War: U.S. Overseas Broadcasting." Tufts University. http://fletcher.tufts.edu/~/media/Fletcher/News%20and%20Media/2009/Sep/Op-Ed/McMahon%2009%2009.pdf.
Mearsheimer, John J. 2001. *The Tragedy of Great Power Politics*. New York, NY: W. W. Norton & Company.
Meijer, Hugo, and Benjamin Jensen. 2018. "The Strategist's Dilemma: Global Dynamic Density and the Making of US 'China Policy'." *European Journal of International Security* 3 (2): 211–234.
Miller, Paul D. 2016. "On Strategy, Grand and Mundane." *Orbis* 60 (2): 237–47.
Morgenthau, Hans J. 1954. *Politics among Nations: The Struggle for Power and Peace*. New York, NY: Knopf.
Mr. Y. 2011. "A National Strategic Narrative." SCIFUN. http://www.scifun.org/Readings/A_National_Strategic_Narrative.pdf.
Mueller, Milton, and Brenden Kuerbis. 2014. "Towards Global Internet Governance: How to End U.S. Control of ICANN Without Sacrificing Stability, Freedom or Accountability." 2014 TPRC Conference Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2408226.
Musgrove, Mike. 2009. "Twitter Is a Player in Iran's Drama." *Washington Post*. http://www.washingtonpost.com/wp-dyn/content/article/2009/06/16/AR2009061603391.html?hpid=topnews.
Narizny, Kevin. 2007. *The Political Economy of Grand Strategy*. Ithaca, NY: Cornell University Press.
NSF. 2004. "On the Origins of Google." National Science Foundation. https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=100660.
Nye Jr., Joseph S. 2011. *The Future of Power*. New York, NY: PublicAffairs.
Obama, Barack. 2010. "National Security Strategy." National Security Strategy Archive. http://nssarchive.us/NSSR/2010.pdf.
Obama, Barack. 2011. "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World." White House. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
Obama, Barack. 2015. "National Security Strategy." National Security Strategy Archive. http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf.
Pritzker, Penny. 2014. "U.S. Secretary of Commerce Penny Pritzker Delivers Remarks at the Internet Corporation for Assigned Names and Numbers Meeting in Los Angeles." Department of Commerce. https://www.commerce.gov/news/secretary-speeches/2014/10/us-secretary-commerce-penny-pritzker-delivers-remarks-internet.
Radu, Roxana, Nicolo Zingales, and Enrico Calandro. 2015. "Crowdsourcing Ideas as an Emerging Form of Multistakeholder Participation in Internet Governance." *Policy and Internet* 7 (3): 362–382.
Raymond, Mark, and Laura DeNardis. 2015. "Multistakeholderism: Anatomy of an Inchoate Global Institution." *International Theory* 7 (03): 572–616.
Sanger, David E. 2012a. "Obama Ordered Wave of Cyberattacks Against Iran." *New York Times*. https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.
Sanger, David E. 2012b. "Mutually Assured Cyberdestruction?" *New York Times*. https://www.nytimes.com/2012/06/03/sunday-review/mutually-assured-cyberdestruction.html.
Sanger, David E. 2018. "Why Hackers Aren't Afraid of Us." *New York Times*. https://www.nytimes.com/2018/06/16/sunday-review/why-hackers-arent-afraid-of-us.html.
Sasse, Ben. 2018. "Senate's Defense Bill Includes Sasse's Cybersecurity Solarium Commission." US Senator for Nebraska Ben Sasse. https://www.sasse.senate.gov/public/index.cfm/press-releases?ID=A75F324A-F7DC-41DE-A0FC-80A472933A28.

Schneier, Bruce. 2014. "Don't Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong." *Atlantic*. https://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612/.

Segal, Adam. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. New York, NY: Public Affairs.

Sepulveda, Daniel. 2014. "Is the Internet Starting to Fracture?" Brookings Institution. https://www.brookings.edu/wp-content/uploads/2014/09/092514_Internet-Fracture_Transcript.pdf.

Shatz, Howard J. 2016. "U.S. International Economic Strategy in a Turbulent World." RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1521/RAND_RR1521.pdf.

Silove, Nina. 2018. "Beyond the Buzzword: The Three Meanings of 'Grand Strategy'." *Security Studies* 27 (1): 27–57.

Sulmeyer, Michael. 2017. "Cybersecurity in the 2017 National Security Strategy." Lawfare. https://www.lawfareblog.com/cybersecurity-2017-national-security-strategy.

Trubowitz, Peter. 2011. *Politics and Strategy: Partisan Ambition and American Statecraft*. Princeton, NJ: Princeton University Press.

US Department of Defense. 2011. "Department of Defense Strategy for Operating in Cyberspace".

US Department of Defense. 2015. "The Department of Defense Cyber Strategy." http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf.

US Department of State. 2012. "Frequently Asked Questions About the World Conference on International Telecommunications (WCIT)." US Department of State. https://2009-2017.state.gov/e/eb/cip/rls/201601.htm.

US Department of State. 2016. "Department of State International Cyberspace Policy Strategy." https://www.state.gov/documents/organization/255732.pdf.

WCIT. 2012. "WCIT-12 Final Acts Signatories." International Telecommunication Union. http://www.itu.int/osg/wcit-12/highlights/signatories.html.

Weber, Valentin. 2017. "Why China's Internet Censorship Model Will Prevail Over Russia's." Net Politics – Council on Foreign Relations. https://www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.

Weitz, Richard. 2018. "Trump's National Security Strategy: We Will Compete." Yale Global Online. https://yaleglobal.yale.edu/content/trumps-national-security-strategy-we-will-compete.

West, Darell M., and Joshua Bleiberg. 2014. "How to Stop the Internet from Breaking Apart." Brookings Institution. https://www.brookings.edu/blog/techtank/2014/10/06/how-to-stop-the-internet-from-breaking-apart/.

World Summit on the Information Society. 2005. "Tunis Agenda for the Information Society." World Summit on the Information Society. http://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html.

Zetter, Kim. 2014. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *Wired*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.