2014

Le cyberspace, c'est moi?: Authoritarian Leaders, the Internet, and International Politics

David P. Fidler
Indiana University Maurer School of Law, dfidler@indiana.edu

Recommended Citation

Fidler, David P., "Le cyberspace, c'est moi?: Authoritarian Leaders, the Internet, and International Politics" (2014). *Articles by Maurer Faculty*. Paper 1673.
http://www.repository.law.indiana.edu/facpub/1673

Le cyberespace, c'est moi?

Authoritarian Leaders, the Internet, and International Politics

by David P. Fidler

OMG! Assad on Instagram?

In late summer 2013, commentary started to crackle over Syrian President Bashir al-Assad's use of Instagram, a social media tool owned by Facebook, to post pictures of himself and his family.[1] The use of Instagram by a dictator—one waging a civil war and accused of using chemical weapons against civilians—prompted criticism of this old-fashioned propaganda digitized for the cyber age.[2] But, Assad is not alone among authoritarian leaders embracing Instagram:

> *Assad is the latest in what one news site has called 'the dictators of Instagram.' Chechen President Ramzan Kadyrov has famously used the social-networking site as a platform to project his very Russian style of masculinity (photo montages of the impossibly barrel-chested despot weight-lifting and posing with wolves and wildcats.) The minions of Ayatollah Khamenei have posted several close-ups of Iran's septuagenarian Supreme Leader on his photo-sharing page.3*

Other authoritarian leaders have shown interest in social media. Vladimir Putin of Russia, Ilham Aliyev of Azerbaijan, and the North Korean government all have Twitter accounts. Before his death in March 2013, Hugo Chavez of Venezuela avidly tweeted to over 4 million followers.[4] Robert Mugabe of Zimbabwe has a Facebook page. Use of social media and the internet by authoritarian leaders can seem like old (and tasteless) wine in new bottles—propaganda delivered through the latest technologies. Authoritarian leaders have long exploited new communication technologies, and their interest in cyber propaganda is more of the same. However, the growing presence of authoritarian leaders in cyberspace might constitute more

David P. Fidler is the James Louis Calamaras Professor of Law at Indiana University's Maurer School of Law, and a Senior Fellow at Indiana University's Center for Applied Cybersecurity Research.

than propaganda. This trend, when viewed with other developments, reflects deeper change in perceptions about the internet in world affairs—a shift from seeing the internet's role in international relations through a domestic lens to viewing cyberspace embedded in anarchical politics among states.

To date, a frequent if not dominant framing of the internet's place in international relations emphasizes domestic issues by looking at how non-state actors use cyberspace to affect domestic regimes, especially within authoritarian governments. Debates over social media's role in the Arab Spring revolutions illustrate this domestic-level focus, as do "internet freedom" initiatives targeting authoritarian governments' behavior in cyberspace. This framing casts the internet as empowering individuals and non-state actors in cyberspace, supporting democratic governance, and threatening authoritarian regimes.

However, this domestic perspective has difficulty explaining authoritarian leaders who increasingly exploit cyberspace for their own purposes. Some commentators noted the oddity of Assad uploading pictures on Instagram where viewers could post responses—certainly a different kind of propaganda than practiced by past authoritarian leaders.[5] Chavez initially branded Twitter an instrument of his enemies—a position consistent with cyberspace being a threat to authoritarian regimes—before he became a prolific tweeter .[6]

An alternative explanation sees Assad's Instagram account and Chavez's tweets intertwined with other developments that challenge framing the internet as a domestic-regime issue in international relations, including efforts by authoritarian governments to increase control over internet activities, shifts in U.S. cybersecurity policy, and Edward Snowden's disclosures about U.S. cyber activities. Together, these developments highlight how *realpolitik* might increasingly characterize cyberspace as part of international relations.

The shift from a domestic-regime focus to an international-system perspective suits authoritarian leaders because it casts cyberspace as less of a threat to their survival and more of an instrument of their power. The shift hurts efforts to connect the internet with democratic governance within states. Draining such democracy preferences helps authoritarian leaders justify their internet activities, especially their emphasis on internal and external security threats. The more the internet operates, and appears to operate, as just another technology subject to power politics, the more authoritarian leaders find cyberspace conducive to their machinations at home and abroad.

CYBERSPACE THROUGH "IMAGES" OF INTERNATIONAL RELATIONS

In examining the causes of conflict. Kenneth Waltz explored whether human behavior (first image), domestic structures of states (second image), or international anarchy (third image) best explained international conflict.[7] These "images" prove useful in exploring cyberspace in international relations because discourse has, roughly speaking, moved from "first image" conceptions focused on the individual into "second image" ideas emphasizing cyberspace's relationship with domestic regimes. Eventually, "third image" readings emerged more strongly and, as this essay argues, gained ascendancy in ways that benefit authoritarian leaders and their regimes.

Beginning at the End of History

Although the internet's origins are in Cold War projects funded by the U.S. Department of Defense, cyberspace only became a prominent issue in the post-Cold War years, especially after the World Wide Web's adoption in the mid-1990s. The internet and cyberspace did not emerge in an environment characterized by great power competition and mistrust. Rather, experts often characterize this period as dominated by U.S. power and ideas—American hegemony and the triumph of liberalism. The internet and cyberspace began in the midst of the "end of history" moment of world affairs.

THE INTERNET AND CYBERSPACE BEGAN IN THE MIDST OF THE "END OF HISTORY" MOMENT OF WORLD AFFAIRS.

This moment encouraged a focus on the individual's relationship with the new technology's impact on human behavior—a "first image" perspective. One iconic example is John Perry Barlow's *A Declaration of the Independence of Cyberspace* from 1996.[8] The *Declaration* rejected government intrusion into cyberspace and claimed individuals around the world "are forming our own Social Contract" without governments and their divisive, jurisdictional baggage.[9] It chastised democratic and authoritarian governments alike for "trying to ward off the virus of liberty by erecting guard posts at the frontiers of Cyberspace."[10] Barlow's vision had no tolerance for distinguishing between domestic regimes or for a system of states defined by the exercise of material power. Instead, individuals would determine cyberspace's fate and "create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before."[11]

People using the internet when the Declaration appeared might not have understood what Barlow envisioned, but what the internet facilitated was unlike anything previously experienced. But, the unique context in which cyberspace emerged was often unaddressed in these years. Imagination had space to roam, unencumbered by "democracy v. dictatorship" debates or threats associated with the harsh logic of structural anarchy.

Second-Image Shift

However, more experience with the internet and cyberspace generated political thinking that emphasized the government and the state. Lawrence Lessig argued that "code is law"—software code shapes behavior as codes of formal law do.[12] Thus, individuals and societies need to use governance mechanisms to ensure that the reliance on software, fueled by commercial interests and market forces, reflects values and interests polities deem important. Lessig focused on domestic politics and governance, reflecting a "second image" understanding of the significance of the internet and cyberspace.

Similarly, debates arose about whether states with fixed boundaries could regulate the internet—a technology that defied borders.[13] An important feature of these debates is the focus on the state and its jurisdiction in a system of states, which raises third-image problems. Questions about regulating internet activities also implicated differences among states on domestic issues, such as freedom of speech. Such differences created the need to examine not only international rules about extraterritorial application of domestic law, but also divergence among countries on individual rights. The internet became important for human rights because internet access supported many rights, such as freedom of association and education, and perhaps constituted a right itself.[14] Discussion about human rights and cyberspace often highlighted how different governments handled the rights-cyberspace relationship.

This "second image" focus put authoritarian regimes under scrutiny and created the perception that the internet's transnational connectivity threatened such regimes. Wider internet access might create communication channels authoritarian governments would have difficulty controlling. Imbuing speech in cyberspace with human rights significance confronted authoritarian predilections to censor speech by opponents. Internet access debates did not focus only on human rights, as illustrated by efforts to address the "digital divide" in development policy. But, human rights permeated this policy area, highlighting authoritarian regimes' attitudes towards civil and political rights and supporting aspirations associated with such rights, especially democratic governance within states.

Third-Image Pushback

Sensing these threats, authoritarian regimes began to challenge how governments and non-state actors framed internet access and cyberspace's political potential. This pushback attempted to shift the focus to international system issues, such as sovereignty, non-intervention, and the exercise of political and military power by dominant states, particularly the United States. Some democratic governments also worried about internet universalism as promoted by the United States, but the central debate was between democracies and authoritarian states.

The authoritarian pushback manifested itself in diplomacy about internet governance. In the early 2000s, China led initiatives to make internet governance more intergovernmental and subject to international law.[15] To this point, internet governance functioned through U.S.-backed multi-stakeholder processes, which produced outcomes not negotiated by states as equals under international law. Authoritarian governments had problems with this model of internet governance because it looked like a U.S. power play aimed at them. The Chinese-led proposals gained sufficient support to cause international talks to reveal a deep lack of agreement. Negotiations about internet governance have, essentially, been deadlocked for over a decade—evidence of the impact China and other authoritarian governments, including Russia, achieved.

Similarly, the Russian government began to draw attention to the military potential the internet created and proposed measures to address dangers of a "cyber arms race."[16] Few countries failed to see that these efforts aimed directly at the perceived advantage the United States had in military cyber power. The United States showed no interest in cooperating with these Russian-led attempts to change the strategic narrative and cast suspicions on U.S. cyber behavior.

Doubling Down

These challenges by authoritarian governments moved policy debates into more polarized and controversial directions. The United States doubled down on the second-image perspective, captured by the emphasis on "internet freedom" in U.S. foreign policy. In January 2010, Secretary of State Hillary Clinton argued that internet technology does not determine how states and non-state actors utilize cyberspace.[17] Rather, the internet is an instrument political systems can bend to their respective wills. Clinton believed the United States should spread a "fifth freedom," the freedom to connect to the internet, by providing opponents of repressive regimes with the means to circumvent controls on, and censorship of, internet use.

THE INTERNET IS AN INSTRUMENT POLITICAL SYSTEMS CAN BEND TO THEIR RESPECTIVE WILLS.

Authoritarian governments doubled down on a third-image approach and stressed "internet sovereignty" as important for stability in the international system. These governments not only pushed this agenda in talks on internet governance but also through an agreement that enshrined this approach. In 2008, the Shanghai Cooperation Organization, a regional security organization composed of authoritarian states, concluded a treaty on international information security, which captured the internet sovereignty perspective and implemented it through an international legal instrument.[18] This strategy continued to cast the main threat as U.S. cyber power, emphasizing not only the U.S. refusal to discuss cyber arms issues but also its violation of the principles of sovereignty and non-intervention through the internet freedom agenda.

Technological Non-Determinism

Perhaps the most significant development under the "internet freedom v. internet sovereignty" clash was authoritarian regimes' realization that increasing internet access did not necessarily make political control of cyberspace impossible. Although not universal among authoritarian governments, many permitted increased internet access. Table 1 lists internet penetration rates for countries often categorized as authoritarian, in 2007 and in 2012, with the increase over this period.

Table 1. Percentage of Individuals Using the Internet

	2007 (%)	2012 (%)	Increase (x)
Azerbaijan	14.54	54.2	3.7
Bahrain	32.91	88	2.7
Belarus	19.7	46.91	2.4
China	16	42.3	2.6
Cuba	11.69	25.64	2.2
Iran	9.47	26	2.7
Kazakhstan	4.02	53.32	13.3
Oman	16.68	60	3.6
Qatar	37	88.1	2.4
Russia	24.66	53.27	2.2
Saudi Arabia	30	54	1.8
Sudan	8.66	21	2.4
Syria*	7.83	24.3	3.1
Tajikistan	7.2	14.51	2.0
Turkmenistan	1.41	7.2	5.1
United Arab Emirates	61	85	1.4
Uzbekistan	7.49	36.52	4.9
Vietnam	20.76	39.49	1.9
Yemen	5.01	17.45	3.5
Zimbabwe	10.85	17.09	1.6

* The number in the 2007 column is the number for 2006.

Source: International Telecommunication Union, 2013

As described below, heightened efforts to control and censor activities in cyberspace often accompanied increased rates of internet use. Leaders in democracies understood the internet had no deterministic logic favoring liberty and democracy. As Secretary Clinton said in her speech on internet freedom, "new technologies do not take sides in the struggle for freedom and progress," but governments do.[19] The notion the internet could support democracy advocacy and reactionary authoritarianism deepened the divide between the internet freedom and internet sovereignty camps.

Cyber Espionage and Cyber Attacks

Another development involves anxieties in the United States and its allies about authoritarian governments' efforts to strengthen and use their cyber power for intelligence and military purposes. Whereas Russia and China had earlier led attempts to produce multilateral initiatives on cyber weapons, events revealed how active these countries were in cyber espionage and cyber attacks. Attention focused on Russia concerning cyber attacks on Estonia in 2007 and during the Russia-Georgia war in 2008.[20] Western experts warned about China's embrace of cyber warfare as a way to counter, frustrate, and defeat U.S. military power.[21] U.S. and European worries about

Chinese cyber espionage, including economic cyber espionage against Western companies, emerged as a major controversy.[22] These developments made power politics among rival states increasingly important in the debate about cyberspace's impact on international relations, a debate previously dominated by the "internet freedom v. internet sovereignty" contest.

Feeding *realpolitik* thinking were revelations in 2010 that the United States, in cooperation with Israel, developed a cyber weapon—the Stuxnet worm—and used it to disrupt and destroy uranium enrichment centrifuges in Iran in order to set back Iran's alleged nuclear weapons program.[23] This incident reinforced concerns many governments had about U.S. cyber power and cyber-weapon capabilities. The Stuxnet attack had nothing to do with promoting democracy in Iran and focused attention on traditional concerns of anarchical international politics, such as war, weapons, and the struggle for national security.

Arab Spring Ambiguity

As Stuxnet magnified *realpolitik* perspectives, the Arab Spring in 2011 rejuvenated internet freedom advocates, whiplashing attention back to the "second image" perspective on the internet's importance in international relations. This renewal began earlier than the Arab Spring with the attention given to use of social media, including Twitter, in the unsuccessful "Green Revolution" following disputed elections in Iran in 2009. Andrew Sullivan's blog headline "The Revolution Will be Twittered" in June 2009 captured the belief that internet-enabled communications threaten authoritarian rulers.[24] Excitement about social media and internet communications as weapons against authoritarian regimes arose as the Arab Spring revolutions in Tunisia, Egypt, and Libya unfolded. However, what contributions social media made to these revolutions remains debated, as does whether revolutions in key countries, especially Egypt and Libya, succeeded or failed. For my purposes, debates about internet-facilitated communications in the Arab Spring focused attention on the threat the internet poses to authoritarian regimes, reinforcing the "second image" lens on cyberspace's place in international relations.

Authoritarianism v. America in Cyberspace

Competition between second and third-image perspectives helps explain authoritarian leaders' increased use of the internet for propaganda and other purposes. Authoritarian regimes pushed back against the interventionism of internet freedom and emphasized Westphalian concerns like sovereignty, non-intervention, threats to national security, and balancing power vis-à-vis the strongest rival state—the United States. Shielded by internet sovereignty, authoritarian leaders perceive the benefits of exploiting cyberspace outweigh the costs.

This conclusion signals that authoritarian regimes believe they can manage the internet's consequences so that cyberspace does not threaten the leadership's grip on power. Put another way, authoritarian leaders have developed sufficient confidence in the capabilities of their regimes to control the politics of internet access to embrace cyberspace for their own purposes. This confidence provides the backdrop for what appears, from the internet freedom perspective, paradoxical—many authoritarian regimes have expanded internet access while also increasing their control over internet use.

Internet Access, Dependence, and Vulnerability in Authoritarian Regimes

In *The Net Delusion: The Dark Side of Internet Freedom*, Evgeny Morozov argued that propaganda, censorship, and surveillance form the "trinity of authoritarianism," and that the internet affects how authoritarian governments engage in these activities.[25] Morozov asserted that the internet makes propaganda, censorship, and surveillance strategies more interconnected than ever before, producing opportunities for authoritarian governments to influence internet usage. Increasing access provides means to heighten surveillance (e.g., monitoring e-mail, social media sites, and blogs), possibilities for more censorship (e.g., restricting access to content through filtering), and avenues to increase propaganda (e.g., using social media to attack opponents and spread pro-government messages). In Freedom on the Net 2013, Freedom House concluded that internet freedom is suffering worldwide because of various forms of internet control, with increased surveillance being the most prominent trend (Table 2).[26]

Table 2. Most Frequently Used Government Internet Control Strategies

1. Blocking and filtering
2. Cyberattacks against regime critics
3. New laws and arrests
4. Paid pro-government commentators
5. Physical attacks and murders
6. Surveillance
7. Takedown and deletion requests
8. Blocking social media and communication apps
9. Intermediate liability
10. Throttling or shutting down service

Source: Freedom House, 2013

Writing for Freedom House, Andrew Rizzardi highlighted efforts authoritarian governments have made to obtain technological capabilities to strengthen their strategies in cyberspace:

> *The 2011 Arab Spring uprisings in Tunisia, Egypt, and Libya demonstrated the power of new media in initiating political change from the bottom up. This did not go unnoticed by authoritarian leaders in other counties, who responded by pursuing advanced technical*

> *infrastructure and expertise with which to monitor and control cutting-edge outlets of dissent like social-networking sites and mobile device. Dictators seeking sophisticated tools of repression need look no further than China, the authoritarian telecommunications hardware store.* [27]

What makes increased internet access and greater authoritarian control of cyberspace possible is individual and societal dependence on the internet. The first and second-image perspectives equate internet access with individual political empowerment and thus seek more and deeper access. Many authoritarian regimes have decided to wager that internet access means dependence on technologies that they can exploit for surveillance, censorship, and propaganda. Such regimes do not perceive the internet as an authoritarian panopticon, but they do not need it to be.

Authoritarian leaders' increasing use of social media is not only propaganda, but also a statement that they do not fear cyberspace because they have learned how to operate in this realm. The strategy involves creating individual, social, and economic dependence on the internet while developing the capacity to exploit dependence for the preservation of power. For opponents of authoritarian regimes, cyber dependence means vulnerability which creates problems if, as proclaimed in the West, internet access leads to transformative political change.

CYBER DEPENDENCE HAS GENERATED WILLINGNESS IN DEMOCRACIES TO VIEW THE INTERNET AND CYBERSPACE INCREASINGLY IN THIRD-IMAGE TERMS.

Cyber Dependence Meets Anarchical Politics in the U.S.A.

Individual, economic, and social dependence on the internet has other implications for international relations beyond allowing authoritarian leaders to tweet with Orwellian intent. Authoritarian regimes have framed internet issues through a third-image lens not only to protect against liberal ideology and interventionist policies but also to provide cover for repression in cyberspace. Interestingly, cyber dependence has generated willingness in democracies to view the internet and cyberspace increasingly in third-image terms. We see this phenomenon in the evolution of U.S. thinking about cybersecurity.

U.S. cybersecurity policy has developed three patterns I call the cyber threat, cyber defense, and cyber technology approaches. The cyber-threat approach involves classifying cyber threats and incidents into traditional categories—crime, terrorism, espionage, and armed conflict—and applying policy prescriptions and legal rules associated with these categories. Although prominent in cybersecurity policy, the cyber-threat approach is criticized for doing little to protect computer systems from intrusions or to prevent attacks from happening in the first place.

This critique informs the cyber-defense approach, which seeks to strengthen cyber defenses in order to prevent damage from cyber threats and to protect against intrusions. Under this approach, building better defenses does not require classifying cyber threats as crime, terrorism, espionage, or war. Rather, it is an "all hazards" strategy to protect against threats from any source. Its raises different policy and legal issues, including questions about the extent to which companies can employ "active defenses." The cyber-defense emphasis also faces criticisms, especially the charge that it places too much confidence in defensive measures in a context where the offense has the advantage.

The third pattern reveals interest in "full spectrum" cyber capabilities to undertake robust defensive measures and offensive actions. This strategy focuses on ensuring that the government develops and maintains powerful technological capabilities for protecting against cyber attacks and, where necessary, engaging in cyber espionage and cyber warfare. Having such capabilities deters adversaries and, if deterrence fails, provides means for defeating threats. The U.S. government's decision to establish a new military command, U.S. Cyber Command (CYBERCOM), to develop the U.S. military's defensive and offensive cyber capabilities demonstrates the importance of this pattern.

More could be said about each approach, but these patterns grapple differently with the threats and vulnerabilities dependence that the internet creates for U.S. national security. U.S. government warnings about cyber intrusions and attacks against government agencies and the private sector underscore the sense in Washington, D.C. that non-state actors, such as cyber-crime organizations or terrorists, and rival powers, such as China, are exploiting the vulnerabilities that American internet dependence creates.

As awareness of the vulnerabilities has grown, U.S. cybersecurity policy has gravitated towards the cyber-technology strategy. Of the three patterns, the cyber-technology approach most closely parallels prescriptions associated with third-image perspectives on international relations—states must meet exogenous security threats with "self-help" measures designed to harness material power to deter and defeat such threats. Increased U.S. attention on cybersecurity in the past decade included efforts to strengthen cyber capabilities in the U.S. intelligence community (e.g., the National Security Agency (NSA)) and the military (e.g., CYBERCOM). In terms of personnel and money, the emphasis on intelligence and military cyber power far surpasses U.S. diplomatic activities on internet freedom. This emphasis brought forth concerns about the U.S. government's "militarization" of cyberspace.[28]

Based on the above, do we see convergence of authoritarian leaders and U.S. officials on viewing the internet and cyberspace predominantly through the lens of power politics? Certainly, authoritarian regimes and the United States have third-image outlooks for different reasons, but a feature of third-image thinking is the discounting of motives in order to concentrate on actual state behavior. The more such a convergence appears plausible, the more this perception benefits authoritarian leaders whose *modus operandi*, internally and externally, is power politics. In this context, the onus is on the United States and other supporters of internet freedom to demonstrate their behavior reflects commitment to democratic principles at home and solidarity abroad, rather than the prescriptions of *realpolitik*.

And then along came Edward Snowden.

The Snowden Affair

At the beginning of June 2013, Edward Snowden, a contractor for the NSA, began disclosing classified information about activities of the NSA and other parts of the U.S. government. From early June until this writing the disclosures continued, and Snowden is likely to leak more. Snowden's disclosures have many features and implications, and this essay does not attempt a comprehensive examination. For my purposes, the Snowden affair's most important feature is its impact on perceptions about U.S. behavior in cyberspace.

The impact has hurt the United States badly. The disclosures have created or reinforced perceptions that the United States acts without constraint because it has the technological capabilities and power to act unilaterally against perceived threats or to gain advantages *vis-à-vis* other nations. The disclosures support the observation that U.S. cybersecurity policy has shifted towards developing and using cyber technologies for offensive and defensive intelligence and military purposes. The leaks suggest a country acting more in line with the tenets of *realpolitik* than internet freedom—the accusation authoritarian governments have made against the United States.

Snowden's disclosures undermine second-image framings of the internet's place in international relations in three ways. First, revelations about the domestic telephony metadata collection program caused controversies, including how "secret jurisprudence" interpretations of federal law affected privacy rights in the United States.[29] Snowden's leaks provided insights into how much NSA surveillance targeting foreign nationals outside the United States catches communications of U.S. persons.[30] For many the scale, intensity, and secrecy of NSA surveillance affecting the communications of U.S. persons made the internet and cyberspace feel less empowering and less free.

Second, various Snowden disclosures revealed substantial U.S. cyber espionage conducted against not only rivals but also allies and friendly countries. At the time of Snowden's first disclosure, the United States had been criticizing China for cyber espionage it conducted against the U.S. government and companies.[31] Snowden subsequently disclosed significant U.S. cyber espionage activities against the Chinese government, companies, and universities, and thus handed China evidence supporting its accusations of American cyber spying in China.[32]

Snowden also disclosed that the United States spied on allies in the European Union.[33] In response, Germany demanded an explanation and terminated its intelligence sharing accord with the United States.[34] Later came revelations about U.S. cyber espionage against Mexico and Brazil, which led the President of Brazil to cancel a state visit to the United States and criticize the United States harshly in her speech to the UN General Assembly in September 2013.[35] The Obama administration's response that every country engages in intelligence gathering only made matters worse, as did telling the Brazilian President that the United States hacked her e-mail as part of U.S. counter-terrorism strategy.[36] For authoritarian leaders, the spectacle of the champion of internet freedom engaging in cyber espionage against democracies and justifying it because "everybody does it" was a political gift.

Third, Snowden disclosed information about U.S. offensive cyber operations by leaking Presidential Decision Directive 20 (PDD 20), finalized in classified form in October 2012.[37] PDD 20 defined different cyber operations the U.S. government would undertake while establishing principles and processes for them.[38] Under PDD 20, President Obama instructed the Executive Branch to "identify potential targets" where,

> *Offensive Cyber Effects Operations (OCEO)...offer a favorable balance of effectiveness and risk compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other U.S. offensive capabilities, and execute those capabilities in a manner consistent with the provisions of this directive.* [39]

PDD 20 defined OCEO as U.S. government operations—other than defensive or espionage activities—undertaken with the intent to enable or produce the manipulation, disruption, denial, degradation, or destruction or computers, computer systems or networks, infrastructure controlled by such systems or networks, or the information located thereon.[40] Although U.S. interest in offensive cyber capabilities was known before PDD 20 was disclosed, its release underscored the seriousness of U.S. interest in offensive cyber power.

Then, Snowden's leak of the classified intelligence budget, the so-called "Black Budget," revealed that U.S. intelligence services carried out 231 offensive cyber operations in 2011, the year before PDD 20's approval.[41] The Black Budget did not illuminate what it meant by "offensive cyber operations," indicating only that "nearly three-quarters were against top-priority targets…such as Iran, Russia, China and North Korea and activities such as nuclear proliferation."[42] However, PDD 20's definition of OCEO provides guidance on what offensive cyber operations in the Black Budget probably entailed. These 231 operations were, in all likelihood, not defensive actions or intelligence gathering activities but were offensive cyber attacks intended to disrupt, manipulate, degrade, or destroy computers or information of foreign targets.

According to the *New York Times*, these operations revealed "how aggressively the United States is now conducting offensive cyber-operations against other nations, even as the Obama administration protests attacks on American computer networks by China, Iran, and Russia."[43] The *Washington Post* noted that "[t]he scope and scale of offensive operations represent an evolution in policy, which in the past sought to preserve an international norm against aggression in cyberspace[.]"[44] Former Deputy Defense Secretary William J. Lynn III explained this shift in a way that underscores the U.S. cybersecurity policy move into "full spectrum" capabilities:

> *The policy debate has moved so that offensive options are more prominent now. I think there's more of a case made now that offensive cyber-options can be an important element in deterring certain adversaries.*[45]

Snowden's disclosures about NSA surveillance of the communications of U.S. citizens and foreign nationals, U.S. cyber espionage, and U.S. offensive cyber operations have marginalized internet freedom as a theme of U.S. cyber behavior, much to the delight of authoritarian regimes. Indeed, Snowden's leaks accumulated into a pile of evidence that the United States treats the internet and cyberspace as an instrument of power politics against allies and adversaries alike—an outcome more consistent with *realpolitik* than liberal thinking in international relations.

Conclusion

In light of Snowden's disclosures, former NSA and CIA Director Michael Hayden admitted in September 2013 that the United States "could be fairly charged with the militarization of the World Wide Web."[46] Asked to justify U.S. behavior, Hayden said U.S. activities are partly justified because the internet originated in the United States, was "quintessentially American," and the United States still carried much global internet traffic.[47] Each reason corresponds to complaints authoritarian governments have long made about American power, and its alleged abuse, within cyberspace.

Even debating whether the United States has militarized the internet serves the interests of authoritarian leaders, who excel at exploiting cyber technologies in the name of power politics. Snowden's disclosures drain away the credibility of second-image narratives about the internet which favor the United States, leaving U.S. policy with an approach resembling what realism would predict for any technology caught in the anarchical politics among states. For many, American cyber exceptionalism after Snowden might appear like unilateralism and militarism, casting shadows on the potential of this "quintessentially American" invention to transform politics within or among nations. This perception, no matter how unfair, plays into the hands of authoritarian leaders, who appear to sense they might finally be leveling the playing field in the international politics of cyberspace. Through increased social-media propaganda, strengthened cyber censorship and surveillance, and the damage Snowden has caused the United States, authoritarian leaders have adapted to the internet and cyberspace, turning what was once threatening into a tool for preserving power and gaining influence.

Le cyberespace, c'est moi? Not yet, but the possibility unfortunately does not seem as ridiculous as once it might have been. No wonder Assad is smiling in his Instagram pictures.

Notes

[1] "According to Assad's Instagram, It's All Smiles in Syria," *Time*, Sept. 5, 2013, http://world.time.com/2013/09/05/according-to-assads-instagram-its-all-smiles-in-syria/.
[2] Jonathan Jones, "The Syrian Presidency's Instagram Account Shows the Banality of Evil," *The Guardian*, Sept. 6, 2013, http://www.theguardian.com/world/2013/sep/06/syrian-presidency-instagram-banality-evil.
[3] Marin Cogan, "Bashar al-Assad's Surreal Instagram Feed," *National Journal*, Sept. 6, 2013, http://www.nationaljournal.com/nationalsecurity/bashar-al-assad-s-surreal-instagram-feed-20130905.
[4] Dan Farber, "Hugo Chavez Dies and the Twitter Town Square Reacts," *CNet.com*, Mar. 5, 2013, http://news.cnet.com/8301-1023_3-57572697-93/hugo-chavez-dies-and-the-twitter-town-square-reacts/.
[5] Megan Garber, "Assad's Bizarre Instagram Account: Propaganda with a Comments Section," *The Atlantic*, Sept. 5, 2013, http://www.theatlantic.com/technology/archive/2013/09/assads-bizarre-instagram-account-propaganda-with-a-comments-section/279396/.
[6] Robert Beckhusen, "How Hugo Chavez Masterfully Trolled the United States on Twitter, TV," *Wired*, Mar. 6, 2013, http://www.wired.com/dangerroom/2013/03/chavez-twitter-troll/.
[7] Kenneth Waltz, *Man, the State and War* (New York: Columbia University Press, 1959).
[8] John Perry Barlow, "A Declaration of the Independence of Cyberspace," Feb. 8, 1996, https://projects.eff.org/~barlow/Declaration-Final.html.
[9] Barlow, "Declaration."
[10] Barlow, "Declaration."
[11] Barlow, "Declaration."
[12] Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 6.
[13] David G. Post, *In Search of Jefferson's Moose: Notes on the State of Cyberspace* (Oxford: Oxford University Press, 2009).
[14] Adam Wagner, "Is Internet Access a Human Right?," *The Guardian*, Jan. 11, 2012, http://www.theguardian.com/law/2012/jan/11/is-internet-access-a-human-right.
[15] Wolfgang Kleinwächter, "The History of Internet Governance," in *Governing the Internet: Freedom and Regulation in the OSCE*, eds. Christian Möller and Arnaud Amouroux (Vienna: Organization for Security and Cooperation in Europe, 2007), 41, http://www.osce.org/fom/26169.
[16] Tom Gjelten, "Shadow Wars: Debating Cyber 'Disarmament,'" *World Affairs* (Nov./Dec. 2010), http://www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament.
[17] Secretary of State Hillary Clinton, "Remarks on Internet Freedom," January 21, 2010, http://www.state.gov/secretary/rm/2010/01/135519.htm.
[18] Shanghai Cooperation Organization, Agreement on Cooperation in the Field of International Information Security, 2008.
[19] Clinton, "Internet Freedom."
[20] Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallin: Center for Cooperative Cyber Defense Centre of Excellence, 2010), 14-35 (Estonia) and 66-89 (Russia-Georgia).
[21] Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges* 7 (2011): 81-103, http://www.securitychallenges.org.au/ArticlePDFs/vol7no2Ball.pdf.
[22] Mandiant, *APT 1: Exposing One of China's Cyber Espionage Units*, Feb. 2013, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
[23] David E. Sanger, *Confront and Conceal: Obama's Secret Wars and the Surprising Use of American Power* (New York: Crown Publishers, 2012).
[24] Andrew Sullivan, "The Revolution Will be Twittered," *The Atlantic*, June 13, 2009, http://www.theatlantic.com/daily-dish/archive/2009/06/the-revolution-will-be-twittered/200478/.
[25] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011).
[26] Freedom House, *Freedom on Net 2013* (Washington, D.C.: Freedom House, 2013), http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf.
[27] Andrew Rizzardi, "The Authoritarian Black Market," June 7, 2013, http://www.freedomhouse.org/blog/authoritarian-black-market.
[28] Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict & Security Law* 17 (2012): 187-209.
[29] Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *The Guardian*, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Peter Wallsten, Carol D. Leonnig, and Alice Crites, "For Secretive Surveillance Court, Rare Scrutiny in Wake of NSA Leaks," *Washington Post*, June 22, 2013, http://articles.washingtonpost.com/2013-06-22/politics/40131927_1_federal-judges-bates-foreign-intelligence-surveillance-court.
[30] Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post*, June 6, 2013,

http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[31] Matt Spetalnick and Steve Holland, "Obama to Press China's Xi to Act Against Cyber Spying," *Reuters*, June 4, 2013, http://www.cnbc.com/id/100790017.

[32] Michael Riley, "Snowden's Leaks Cloud U.S. Plan to Curb Chinese Hacking," *Bloomberg.com*, June 30, 2013, http://www.bloomberg.com/news/2013-07-01/snowden-s-leaks-cloud-u-s-plan-to-curb-chinese-hacking.html.

[33] Josh Levin and Catherine E. Sholchet, "Europe Furious, 'Shocked' by Report of U.S. Spying," *CNN*, July 1, 2013, http://www.cnn.com/2013/06/30/world/europe/eu-nsa/index.html.

[34] Laura Smith-Spark and Stefan Simons, "Germany Ends Information Sharing Pact with Britain, United States," *CNN*, August 3, 2013, http://www.cnn.com/2013/08/03/world/europe/germany-uk-privacy/index.html.

[35] Reuters, "NSA 'Spied on Communications' of Brazil and Mexico Presidents," *The Guardian*, September 2, 2013, http://www.theguardian.com/world/2013/sep/02/nsa-spied-mexico-brazil-presidents; Julian Borger, "Brazilian President: US Surveillance a 'Breach of International Law,'" The Guardian, September 24, 2013, http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

[36] Tom Cohen and Michael Pearson, "All Nations Collect Intelligence, Obama Says," *CNN*, July 2, 2013, http://www.cnn.com/2013/07/01/world/europe/eu-nsa/index.html; Gerald Jeffris, "Brazil President Says Spying Not Justified by Terrorism Concern," *Wall Street Journal*, September 24, 2013, http://online.wsj.com/article/SB10001424052702304213904579095210325139486.html.

[37] Glenn Greenwald and Ewen MacAskill, "Obama Orders US to Draw Up Overseas Target List for Cyber-Attacks," *The Guardian*, June 7, 2013, http://www.theguardian.com/world/2013/jun/07/obama-china-targets-cyber-overseas.

[38] Presidential Decision Directive 20/PDD-20, U.S. Cyber Operations Policy, October 2012, http://epic.org/privacy/cybersecurity/presidential-directives/presidential-policy-directive-20.pdf.

[39] Presidential Decision Directive 20, 9.

[40] Presidential Decision Directive 20, 2.

[41] Barton Gellman and Ellen Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011, Documents Show," *Washington Post*, August 30, 2013, http://articles.washingtonpost.com/2013-08-30/world/41620705_1_computer-worm-former-u-s-officials-obama-administration.

[42] Gellman and Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011."

[43] David E. Sanger, "Budget Documents Details Extent of U.S. Cyberoperations," *New York Times*, August 31, 2013, accessed October 7, 2013, http://www.nytimes.com/2013/09/01/world/americas/documents-detail-cyberoperations-by-us.html?_r=0.

[44] Gellman and Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011."

[45] Gellman and Nakashima, "U.S. Spy Agencies Mounted 231 Offensive Cyber-Operations in 2011."

[46] Andrea Peterson, "Former NSA and CIA Director Says Terrorists Love Using Gmail," *Washington Post*, September 19, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/15/former-nsa-and-cia-director-says-terrorists-love-using-gmail/.

[47] Peterson, "Former NSA and CIA Director Says Terrorists Love Using Gmail."