# Going Dark

Summer_2019
Vol_6 No_1

FLETCHER SECURITY REVIEW
OMNIBUS SECURITAS

# Going Dark

## How Living in a 21st Century World Affects Security and Geopolitics

Summer 2019
Vol. 6 No. 1

## Leadership

Editor-In-Chief
Kacie Yearout

Managing Editor
Annalise Burnett

Creative Director
Keifer Chiang

## Policy

Senior Policy Editors
Chloe Logan
Lauren Michaels

Staff Editors
Matthew Bendure
Swati Bisen

## Book Reviews & Interviews

Senior Book Reviews & Interviews Editors
Ryan Rogers
Maia Brown-Jackson

Staff Editors
Akshobh Giridharadas
Gauri Gupta
Divya Prabhakar

## Current Affairs

Senior Current Affairs Editors
Arthur S. Montandon
Tawni Sasaki

Staff Editors
Annie Su
Moriah Graham
Andrew Hogan

## Digital

Team Lead
Senjuti Mallick

Staff
Kendra Poole
Lukas Bundois

## Business Outreach

Business Director
Tom Rodems

## About FSR

The Fletcher Security Review (www.fletchersecurity.org) is a print and online journal managed and edited by students at Tufts University's Fletcher School of Law and Diplomacy. At FSR, we aim to build on the school's strong traditions of marrying theory with practice and fostering close interdisciplinary collaboration to act as an incubator for unique perspectives across a broad range of security issues. We hope to provide our contributors a forum for advancing new theses or for innovative approaches to established ones. Because we believe in publishing the work of established and emerging scholars, practitioners, and analysts on topics and from perspectives deserving greater attention, FSR can serve as a distinctive medium in the security field.

## Advisory Board

Richard Shultz
Professor of International Politics and Director, International Security Studies Program

Kelly Sims Gallagher
Professor of Energy and Environmental Policy and Director, Center for International Environmental Resource Policy

Daniel W. Drezner
Professor of International Politics and Nonresident Senior Fellow at the Brookings Institution

Monica Duffy Toft
Professor of International Politics and Director, Center for Strategic Studies

Robert Pfaltzgraff
Shelby Cullom Davis Professor of International Security Studies

## Thank You to Our Sponsors

ISSP
INTERNATIONAL SECURITY STUDIES PROGRAM

Russia and Eurasia Program
U.S.-RUSSIA RELATIONS INITIATIVE

## Contact Us

Address Letters to:
Editor in Chief, Fletcher Security Review
The Fletcher School
160 Packard Avenue, Medford, MA 02155

Or by Email:
Editor in Chief, Fletcher Security Review
fletchersecrev@gmail.com

## Information for Authors

Please send submissions to fletchersecrev@gmail.com. All submissions should be sent as a Microsoft Word file. Short articles should be 1,500 to 2,000 words and long articles should be 3,000 to 5,500 words.

## Referencing

Last Name, First Initial. Middle Initial. (2019). Article Title. *The Fletcher Security Review*, 6(1), Pages.

## Credits

Cover Design by Keifer Chiang

# Editor's Note

Technology touches nearly every part of our daily lives, and *Fletcher Security Review*'s Summer 2019 issue examines the influence technology has on security, whether it be IT or military technology. As editor-in-chief, I encouraged our editors to go beyond the assumptions, and I believe this edition both evaluates and investigates the complexity of technology and security.

This edition was possible thanks to the hard work of many, particularly Annalise Burnett, the managing editor. Annalise assisted in many decisions and willingly took on challenges, in addition to being an excellent editor. As the future editor-in-chief, I am confident she will bring the journal further success. I also must highlight the incredibly talented Keifer Chang, the creative director for *FSR*, for his keen eye and dedication to producing a modern academic journal.

The senior staff members have routinely gone above and beyond in their positions. Thank you to Chloe Logan, Lauren Michaels, Arthur Montandan, Tawni Sasaki, Maia Brown-Jackson, Ryan Rodgers, and Senjuti Mallick for your dedication and leadership. This journal is possible thanks to the hours they spent working with our contributors and encouraging staff editors.

Professor Richard Shultz and the International Security Studies Program have once again generously funded this journal, allowing us to focus on the quality of the articles. The Fletcher Russia and Eurasia program has also provided the critical funding needed to design this journal. Thank you both for your continued support.

I have been honored to work with so many talented people and read so many interesting articles as editor-in-chief. I have aimed to produce a journal that looks critically at the security issues we face today. Thank you to the contributors that have critically evaluated issues facing our world today, and I hope some of your insights and solutions result in a more secure world. I hope you enjoy this summer's edition of *Fletcher Security Review*.

Kacie Yearout
Editor-in-Chief

Military Technologies

National Security

Cyberspace

> Today, Moscow firmly understands the need to base the development of its armed forces on the creation of modern weapon systems

**Trans-Baikal, Russia.** Review of troops, held after Vostok-2018
(The Russian Presidential Press and Information Office / CC BY 4.0)

# The Rise of Russia's Hi-Tech Military

Samuel Bendett

## INTRODUCTION

Following the end of the Cold War, the Russian Federation lagged behind the United States in terms of advanced technology in warfighting. However, after substantial spending on modernization starting in 2008, the Russian military and the nation's defense sector have been making great strides at developing remotely operated and autonomous technologies and integrating them in their tactics and combat operations. Russia is also starting to invest in Artificial Intelligence (AI) development with specific military applications. These developments affect the ability of the United States to meet the goals in its new National Security Strategy; in order to meet its stated December 2017 objective of renewing American competitive advantage in key military areas, the United States should be aware of key adversarial developments such as Russia's emerging unmanned, autonomous, and AI capabilities, and prepare itself in terms of appropriate capabilities, tactics, and plans.

## DEFINING THE THREAT…

The Russian military establishment has discussed potential threats over a number of years, seeking to analyze both likely adversary and domestic capabilities. Such deliberations gained greater importance following Russia's own military experience in Syria since 2015, when the Russian government and its generals began noting advanced technology like autonomous and robotics systems as significant mission multipliers. In fact, Russian military experience in Syria has proved crucial in testing out concept of operations (CONOPS) and tactics/techniques/procedures (TTPs ) for future conflicts. For example, in 2017, Russian President Vladimir Putin said that autonomous robotic systems can cardinally change the way Russia's military operates, calling the use of military robotic systems a major pivot in the right direction.[1] In March 2018, General Valery Gerasimov, the chief of the General Staff of the Russian Armed Forces, noted that Syrian conflict represented the "contours of future war."[2] He called the Syrian experience "priceless" for Russia's military,[3] pointing out that the United States and its allies used a wide arsenal of high-tech weapons there, such as drones, satellites, and various robotic systems, alluding that the Russian military was learning from its potential adversary and trying out similar tactics and technologies in combat.[4]

Such tactics and technologies were also reviewed in 2016 by Putin, who said that the operation in Syria had demonstrated "qualitatively increased capabilities" of the Russian army and navy.[5] In December 2018, Gerasimov noted that the main emphasis in the training of his country's military is placed "on the potential opposition to the high-tech enemy," without explicitly naming the American or NATO forces.[6] "…We teach the troops to conduct combat operations with a high-tech adversary equipped with the most modern weapons, under the conditions of conducting all types of reconnaissance and electronic exposure, massive use of aircraft and high-precision weapons," the military commander said.[7]

Today, Moscow firmly understands the need to base the development of its armed forces on the creation of modern weapon systems: advanced complexes ensuring the use of the latest technologies, such as military robotic systems and unmanned aerial and naval autonomous systems.[8] According to Dmitry Rogozin, the former deputy prime minister who currently heads the Russian space agency Roscosmos, the country's State Armament Program for 2018-2025 addresses this need by being "inherently innovative," and by aiming to create "intelligent" weapons, automatic control systems, and new communications and intelligence systems.[9] In particular, the program addresses the development of ground-based automated systems and unmanned aerial vehicles for Russia's armed forces.[10]

## …AND MEETING THE CHALLENGE

Today, the Russian military's burgeoning fleet of unmanned aerial vehicles (UAVs) provides a key mission multiplier. Currently, the Russian military has more

**Russian unmanned aerial vehicle** at MAKS-2011 (Vitaly V. Kuzmin / CC BY-SA 4.0)

than 2,100 unmanned aerial vehicles throughout its services, according to the Ministry of Defense (MOD).[11] This makes the Russian unmanned aerial fleet one of the largest in the world, behind the American fleet (at more than 10,000 UAVs) and possibly larger than the Chinese fleet.[12] Moreover, starting in 2019, under the defense procurement plan, the Russian military will get more than 300 short-range UAVs annually.[13] While until recently Russia lagged behind other powers such as the United States, Israel, and China in developing long range combat unmanned aerial platforms, Moscow has proven very adaptable in using its existing capabilities in its military TTPs.

The vast majority of Russian military drones are unarmed, lightweight, short ranged, and relatively inexpensive. The workhorse of the Russian UAV fleet today is a domestically-produced Orlan-10, with a range of up to 120 km, forming nearly half of all UAVs flown by the Russian military.[14] With a range of up to 250 km, medium altitude, long endurance (MALE) drones known as Forposts are Russia's current longest-ranged UAV. The Forpost-class UAV is itself an older Israeli design assembled in Russia under a license agreement.[15]

Although Russian drones have primarily been used to support land-based targeting, the Russian military is developing unmanned aerial systems for use in a number of different missions, such as an intelligence, surveillance, and reconnaissance (ISR) and targeting platform for tanks,[16] artillery, and ship-based missiles. Other disparate examples include UAV support to the security of Russia's mobile Strategic Missiles Forces and for monitoring conditions at sea.[17]

The Syrian campaign proved unprecedented for Russia in fielding unmanned aerial platforms. According to the MOD, Russia's drones have flown at least 23,000 sorties and logged 140,000 hours supporting intelligence, surveillance, reconnaissance, and target acquisition missions, far exceeding the number of sorties flown by manned aircraft in that campaign.[18]

## …ADDRESSING KEY CAPABILITY GAPS IN THE AIR…

December 2018 was marked by a series of key announcements from the MOD about the country's growing unmanned combat aerial systems capabilities.[19] Going into Syria in 2015, Russia was lacking a key combat element — the ability to hit targets quickly following their identification and confirmation, one of the key functions of unmanned combat aerial vehicles (UCAVs) around the world today. Moscow's experience in Syria underscored that point; despite fielding a large number of ISR drones that enabled Russia to be more

**Moscow, Russia.** The Ministry of Defense of the Russian Federation (Ohnedich / CC BY-SA 4.0)

precise in combat, the majority of targets were hit by manned aviation or manned artillery forces. Hence the push today to field an entire lineup of strike-capable UAVs for a diverse range of missions. Recently, Putin announced that key propriety areas for Russia's military in 2019 include an emphasis on "robotic systems" development alongside artificial intelligence.[20]

Over the past decade, the lack of key expertise and high-tech components needed to build long-range combat and strike UAVs have challenged the Russian defense industry. Delays in deliverables also plagued the efforts by Russian organizations and enterprises that pioneered work on UAV systems in the country. As a result, the entire schedule of many projects was delayed by several years. A good example is Simonov Design Bureau, the company originally in charge of building a long-range high altitude, long endurance (HALE) UAV known both as Altair and Altius.[21] This was one of the most ambitious UAV projects in Russia - the objective was to build an indigenous drone capable of carrying up to 2.5 tonnes of cargo, equipment, and weapons to a distance of up to 6,000 miles. Earlier estimates that this UAV would be fully operational by 2018 did not prove true. After Simonov depleted its budget allocated for the project and asked MOD for more funding, the defense establishments transferred key parts of the project to UZGA defense enterprise. The new managing company is the same one responsible for assembling Forpost UAVs for the military. In December 2018, MOD promised that the Altius would take to the skies in 2019 - given the fact that Simonov has produced a prototype that has already flown, this promise may indeed materialize.[22] The real issue will be the quality of that test flight — whether Altius will fly as intended and with the right amount of key equipment.

The MOD also mentioned work on a strike version of the Forpost mid-range drone. Capable of distances up to 250 kilometers, it is currently Russia's longest-ranged drone. Under the earlier license agreement with Israel, this UAV could only be assembled as an ISR version. The Russian military values this particular unmanned vehicle and has long wanted to turn it into something more than an extra pair of eyes in the sky. Today, UZGA, the defense enterprise responsible for assembling it in Russia, claims that the "Russified" version of Forpost is already available and carries Russian-made components so that no further cooperation with and dependence on Israel would be necessary.[23] Adding strike capabilities to Forpost would give Russia an immediate ability to hit targets within a 250 kilometer range — in other words, giving it the ability to strike most adversary targets in Syria where Russian forces are still conducting

**Russian** Global Navigation Satellite System (GLONASS) spacecraft (Vitaly V. Kuzmin / CC BY-SA 4.0)

operations. Given that Forpost itself is an older UAV model, it is likely that the Russian military will use it as a test bed to further refine its UAV manufacturing abilities, as well as to test indigenous munitions.

The MOD likewise named Orion UAV as another unmanned vehicle that is set to fully see the light of day in 2019.[24] Orion shares similar characteristics with Forpost, such as a range of 250 kilometers.[25] It is possible that its range could be extended further – current Orion versions are showcased as ISR models, but there have been discussions that an armed version could be offered for export. This particular UAV has similar design features to the ever-growing family of unmanned aerial vehicles all over the world; it bears close resemblance to the American RQ-9 Reaper and Chinese CH-4 and Ch-5 drones, as well as to the Iranian Shahed and Turkish Anka UAVs.

The Russian Ministry of Defense also mentioned Ohotnik UCAV.[26] The Ohotnik is the most intriguing and interesting project of its kind in Russia. Originally started around 2011-2012, this UAV has also been delayed by a number of years. In the fall of 2018, MOD carried out the first "taxiing" test, where an Ohotnik prototype was accelerated on the runway to test its engine. For 2019, the Russian defense establishment has promised a test that will include a short-duration "jump" – the UCAV will rise ever so briefly above the tarmac to test its launching and landing capabilities. It will be Russia's heaviest and fastest UAV when fielded, but additional testing and evaluation needs to take place in order for this unmanned system to be fully functional. Its high speed - up to 1000 km/hr, and heavy weight, projected to be at up to 20 tonnes - means that a host of aerodynamic, electronic, and high-tech issues need to be worked out.[27] Given the delays experienced with the Altius project, the MOD should probably be more conservative with Ohotnik estimates. However, the very appearance[28] of the Ohotnik rising in the air - a stealthy blended-wing design - will be a powerful PR coup for a country that has lagged behind nations such as the United States, Israel, and China in actual UCAV development and combat use.

There are other UAV platforms that the Russian defense establishment has been testing and evaluating. One of such systems is the Korsar MALE UAV, which the Russian military exhibited at the May 9 Victory Parade in Moscow.[29] Today, the Korsar is ranging up to 180 km, and it too could have an extended operational range in the near future.  Supposedly, this UAV was actually tested in Syria.[30] The Russian military is also evaluating the Carnivora UAV with the capacity to hunt smaller adversary UAVs and deliver munition strikes.[31] All these UAVs, if and when fielded as planned and as advertised, will give Russia the capability to strike targets at a range anywhere from 250 kilometers up to several thousand kilometers. Moreover, these and other unmanned aerial systems in development are designed with the ability to operate in an environment when radio-electronic signals are suppressed, as well as to navigate without GPS or GLONASS.[32] Such technology capabilities could give the Russian military the flexibility it has long sought –

for example, its Syrian actions depended on manned airborne assets conducting deep-strike against designated targets, which in turn depended on an extensive logistics and infrastructure network to support such missions. Launching long-range UCAVs that would take off from Russian (or Russian-allied) territory would exponentially increase MOD's ability to conduct missions in the near abroad and possibly around the world. Of course, that would depend largely on the domestic defense sector actually delivering what was initially promised, something that some UAV projects have so far struggled to accomplish.

Moreover, while the Russian military has gained extensive experience operating a wide range of close- and short-range UAVs and has commenced force-wide training and usage of these unmanned systems, operating large and heavy drones would be a different story. This kind of technology requires different training, as well as different logistical and infrastructure support. Getting these UCAVs into the military will require a change to existing CONOPS and TTPs, something that will take time as the Russian military will need to become familiar with a different level of technological sophistication. Still, these UAVs are finally moving past the prototype stage. With the Ministry of Defense paying very close attention to these projects, these designs' announced 2019 debut is likely; however, their eventual acquisition is still years away. Nonetheless, Russia's potential "high-tech adversaries" have been put on notice, and the time when the United States military reigned unchallenged with its MALE and HALE UAVs is nearing its end. Russian UCAV plans will have important implications for the way Moscow thinks about, designs, tests, and eventually conducts warfare.

### …ON LAND AND AT SEA…

When it comes to Russia's unmanned ground systems (UGVs), the country is developing an entire lineup to meet various combat needs.[33] These include small systems for better ISR to large, tank-sized vehicles loaded with long-range, anti-tank and anti-aircraft weapons. While most of them are still undergoing testing and evaluation, some have already undergone a trial by fire. Russia took its heaviest UGV, Uran-9, to Syria for "near-combat testing", where the users and developers discovered that it failed along all major criteria – from engine to targeting to firing to communications to other key systems.[34] This rather unexpected problem nonetheless resulted in the emergence of a possible UGV CONOPS for the Russian military – the use of such system in a one-off attack role, a possible "kamikaze" strike squad that identifies and targets adversary positions, weapons, and personnel. How that will actually play out is unclear given the rather expensive price tag for such weapons in terms of material and man-hours needed to build it, but the Russian military is keen to explore this in the coming years and has already announced that this UGV will be officially acquired by the armed forces.[35] While another combat UGV, Soratnik, may have also been tested in Syria,[36] the military will soon start acquiring non-combat demining UGVs – Uran-6, Scarab and Sphere – that have served with the country's military in Syrian combat.[37]

**Vikhr** reconnaissance-assault unmanned ground vehicle (Vitaly V. Kuzmin / CC BY-SA 4.0)

At sea, the Russian military-industrial complex is likewise developing a range of unmanned underwater/surface vehicles (UUV/USV) for the navy. Official announcements state that no fewer than 17 designs are currently in development,[38] while some UUVs like Galtel were already used in Syria for sea-floor mapping and monitoring.[39] The Russian Navy is keen on using UUV and USV in ISR, monitoring, demining, anti-submarine, and target acquisition roles,[40] while such vehicles will also help in exploring and guarding the country's Arctic domain.[41]While the Western media picks up on "big-ticket" items like Poseidon nuclear-powered and nuclear-equipped UUV,[42] the rest of the country's UUV/USV work that does not get much attention overseas is marked by "import-substitution" drive, referring to replacing imported technology with domestic technology. While government claims that such "substitution" is well on its way, much remains to be seen in terms of the Russian technological potential actually stepping up to deliver promised results. As with some UAV projects, certain delays and schedule adjustment would be inevitable, but given Moscow's desire to once again be a peer competitor in the maritime domain, the pressure from the Kremlin and the MOD may yield desired outcomes.

## ...AND GETTING SMART WITH AI.

The overall AI development in the Russian Federation is rapidly growing, both across the private sector as well as the government and the country's military. Just recently, Putin remarked that, to him, the most interesting area of national research involves AI, along with genetics.[43] Today, a lot of AI-related research takes place at the Russian Ministry of Defense, which is dedicating financial, human, and material resources across its vast technical, academic, and industrial infrastructure. Russia's private-sector AI development is also enjoying a revival, due in large part to the nation's overall strong STEM academic background that is so conducive to high-tech development.

The most significant defense-oriented effort is taking shape at the Advanced Research Foundation (ARF - Фонд перспективных исследований (ФПИ)). The Russian government established ARF as an analogous to the United States' DARPA (Defense Advanced Research Project Agency) in October 2012.[44] Today, ARF encompasses[46] research laboratories.[45] On March 20, 2018, ARF announced that it had prepared proposals for the MOD on the standardization of AI development, which includes the following key areas:[46] image recognition, speech recognition, enabling control of autonomous military systems, as well as AI's support for weapons life-cycle.

ARF announced these principles in March 2018 at a major forum titled "AI: Problems and Solutions."[47] This event was organized by the MOD, Ministry of Education, and the Russian Academy of Sciences in order to advance proposals aimed at the mobilization of the state

**Tula, Russia.** Meeting on the work of the Advanced Research Foundation (The Russian Presidential Press and Information Office / CC BY 4.0)

**Moscow, Russia.** Presentation of the ERA innovation technopolis (The Russian Presidential Press and Information Office / CC BY 4.0)

and the scientific community toward AI work.[48] In his address to the conference participants, Russian Defense Minister Sergei Shoigu specifically called for the country's civilian and military designers to join efforts to develop artificial intelligence for the nation's technological and economic security."[49] This international symposium's key result was the publication of the 10-step recommendation "roadmap" for AI development in Russia.[50] This roadmap outlined proposed public-private partnerships and short- to medium-term developments that should be undertaken. It called for multiple initiatives that included: an AI and Big Data consortium, building out the national automation expertise and creating a state system for AI training and education, and running military games that will determine the impact of artificial intelligence on military operations at the tactical, operational, and strategic levels.

One of the roadmap's most important proposals came from the Russian Academy of Sciences and the ARF. It called for the establishment of a National Center for Artificial Intelligence (NCAI)."[51] The MOD, as one of the driving forces behind such proposals, claimed to have enough academic know-how to start building out realistic AI capabilities. During the March 2018 conference, Russian Deputy Minister of Defense Nikolai Pankov stated that, "of the 388 scientific research institutions (in the Ministry of Defense of Russia), 279 are concentrated in military schools, and most of them are actively engaged in research in the field of artificial intelligence, robotics, military cybernetics, and other promising areas."[52] To underscore an emerging systemic approach towards artificial intelligence development in the country, Russian civilian organizations and technical centers are expected to release an AI roadmap in mid-2019 in order to accelerate and "digitize" the domestic economy.[53] Two key organizations involved in the March 2018 efforts are part of this new plan: the military-affiliated ARF and the Russian Academy of Sciences. Moreover, Putin is pushing his government to come up with a national AI roadmap this year that would presumably draw on previous efforts to develop an overarching national strategy for artificial intelligence development.[54]

The MOD's efforts to build out infrastructure enabling AI development are also exemplified by the creation of a military innovation "technopolis" in Anapa, on the Black Sea Coast, called "ERA."[55] This high-tech city will consist of a science, technology, and research development campus, where the military and the private sector can work together. The ERA will host an "AI Lab" – another major item in the 2018 "roadmap" that will be supported by the MOD, Federal Agency for Scientific Organizations, Moscow State University, and the Russian Academy of Sciences, and will be staffed by soldiers from the scientific companies and regiments.[56] Work on

ERA began in 2018 and is projected to be completed by 2020, when it will be staffed by around 2,000 researchers. Russian military is already sending soldiers from its science and technology detachments to start work there.[57]

Currently, the Russian military is working on incorporating elements of AI in its various weapons systems.[58] The Russian military has also highlighted the importance of AI in data collection and analysis in order to facilitate information processing. Specifically, in March 2018, then-Deputy Defense Minister Borisov stated that AI development is necessary to effectively counter opponents in the information space and to win in cyberwars.[59] Given Russia's ongoing and robust efforts in information warfare, it is expected that AI would play a more prominent role in the coming years. Russia's civilian AI developments in image and speech recognition may also be incorporated into defense and security applications down the line. It is also important to note that at this point, there have been no official statements that alluded to any dissent in the Russian AI community against the use of its technologies for military purposes, in contrast to the ongoing dispute at Google on its role in the American defense sector.[60]

## CONCLUSION

The Russian defense sector is gearing up for a long-term high-tech competition with its perceived adversaries – namely, the United States and NATO. In Moscow's viewpoint, gone are the days when the country's military looked with envy at the latest Western military actions around the world. While certain issues remain, the Russian MOD and its military-industrial sector are more in sync than at any point since 1991. Beginning in 2012, the MOD established departments[61] and centers[62] dedicated to developing unmanned and robotic technologies and creating a systemic approach that aims to streamline and facilitate these weapons from their initial development to the eventual (or potential) acquisition. This development of new weapons is well underway – technologies capable of extending Russian military's reach in combat give it a better situational awareness and save soldiers' lives. Unmanned aerial, ground, and sea-based systems are key in this process. Moreover, Moscow wants to eventually endow such systems with some form of AI for more effective combat roles. Still – while the Russian defense sector has proven capable in designing a diverse suite of unmanned systems, the government will have to reconcile the budgetary issues and combat realities against the military's acquisition wish lists, which will affect what "robotic complexes" are ultimately purchased and fielded. Nonetheless, the past seven years of developments across the Russian defense sector indicate that as the Russian military matures to more advanced tech levels, the United States would have to eventually face a more effective and capable adversary. This will challenge the U.S. military to develop new CONOPS in countering what it has not done for many years – a peer adversary eager to field breakthrough and advanced military technology in combat.

[1] Путин: боевые роботы могут существенно изменить армию России. Izvestia, January 26, 2017, <https://iz.ru/news/660335>.
[2] Aleksey Zakvasin, "«Контуры войны будущего»: как российская армия готовится к конфликтам нового поколения," RT, March 27, 2018, <https://russian.rt.com/russia/article/496787-gerasimov-voina-novoe-pokolenie>.
[3] Ibrahman, Pandora Open, February 5, 2017, "Генерал Герасимов: сирийский опыт — бесценная школа для российских войск," <https://pandoraopen.ru/2017-02-05/general-gerasimov-sirijskij-opyt-bescennaya-shkola-dlya-rossijskix-vojsk/>.
[4] Aleksey Zakvasin, "«Контуры войны будущего»: как российская армия готовится к конфликтам нового поколения," RT, March 27, 2018,<https://russian.rt.com/russia/article/496787-gerasimov-voina-novoe-pokolenie>
[5] "Упор на интеллект. Россия откажется от модернизации старого оружия," RIA Novosti, May 20, 2017, <https://ria.ru/defense_safety/20170520/1494729459.html>
[6] Ivan Petrov, "Армию России готовят к противостоянию с высокотехнологичным противником," Rossiyskaya Gazeta, December 5, 2018, <https://rg.ru/2018/12/05/armiiu-rossii-gotoviat-k-protivostoianiiu-s-vysokotehnologichnym-protivnikom.html>.
[7] Ibid.
[8] В. А. Киселёв, "К каким войнам необходимо готовить Вооруженные Силы России," Voennaia mysl' 3  (March 2017): 37-46, <https://dlib.eastview.com/browse/doc/48395296>.
[9] "Упор на интеллект. Россия откажется от модернизации старого оружия," RIA Novosti, May 20, 2017, <https://ria.ru/defense_safety/20170520/1494729459.html>.
[10] Ibid.
[11] "За шесть лет в российскую армию поступили более 1800 беспилотников различных классов," Russian News Agency, November 5, 2018, <https://tass.ru/armiya-i-opk/5758113>.
[12] The exact UAV numbers in the American and Chinese militaries are hard to ascertain from the open sources. However, this 2014 Wikipedia entry <https://en.wikipedia.org/wiki/UAVs_in_the_U.S._military> puts the American fleet at more than 10,600 systems. Chinese UAV numbers are also not readily available, though this Wikipedia page <https://en.wikipedia.org/wiki/List_of_unmanned_aerial_vehicles_of_China#Comprehensive_list> lists several hundred UAV models and notes numerous companies working on unmanned aerial vehicle developments, enabling the conclusion that Beijing may have at least several hundred UAVs in its military forces.
[13] "Reconnaissance and attack drones to arrive for Russian Army from 2019," Russian News Agency, December 18, 2018, <http://tass.com/defense/1036662>.
[14] "«Тахион», «Орлан» и «Элерон»: зачем в ВДВ России создают подразделения беспилотной авиации," RT, 29 May 2018, <https://russian.rt.com/russia/article/517579-vdv-bespdesantniki-bespilotniki-podrazdelenija-sozdanijeilotniki>.
[15] Nikolay Surkov, Aleksey Ramm, "Русский «Форпост» поступит в войска в 2019 году,"RT, April 28, 2018, <https://iz.ru/736932/nikolai-surkov-aleksei-ramm/russkii-forpost-postupit-v-voiska-v-2019-godu>.
[16] Mil.ru, September 23, 2018, "«Форпост» обеспечил наступление танкового соединения в ходе учения на Урале," Zvezda, <https://tvzvezda.ru/news/forces/content/201809231716-mil-ru-yme83.html>.
[17] Alexander Kruglov, Evgeny Dmitriev, "ВМФ расширил использование дронов," Izvestia, August 17, 2018, <https://iz.ru/775543/aleksandr-kruglov-ev-

genii-dmitriev/vmf-rasshiril-ispolzovanie-dronov>.

[18] “В Минобороны назвали число беспилотников в российской армии,” Izvestia, July 6, 2018, <https://iz.ru/763798/2018-07-06/v-minoborone-nazvali-chislo-bespilotnikov-v-rossiiskoi-armii>.

[19] “Russia’s heavy strike drone to make debut flight in spring,” Russian News Agency, December 19, 2018, <http://tass.com/defense/1036780>.

[20] “Путин рассказал о внедрении искусственного интеллекта в военное дело,” Izvestia, May 18, 2018, <ttps://iz.ru/745150/2018-05-18/putin-rasskazal-o-vnedrenii-iskusstvennogo-intellekta-v-voennoe-delo>.

[21] Patrick Tucker, “The Designer of Russia’s First Armed Drone Is Under Arrest,” Defense One, April 25, 2018, <https://www.defenseone.com/technology/2018/04/designer-russias-first-armed-drone-under-arrest/147751/>

[22] Zeeshan Aziz, “Russia's Heavy Lift Drone Altius To Make Maiden Flight In 2019 - Defense Ministry,” UrduPoint, Decenber 19, 2018, <https://www.urdupoint.com/en/world/russias-heavy-lift-drone-altius-to-make-maid-510638.html>.

[23] Nikolay Surkov, Aleksey Ramm, “Русский «Форпост» поступит в войска в 2019 году,” Izvestia April 28, 2018,<https://iz.ru/736932/nikolai-surkov-aleksei-ramm/russkii-forpost-postupit-v-voiska-v-2019-godu>.

[24] “Reconnaissance and attack drones to arrive for Russian Army from 2019,” Russian News Agency, December 18, 2018, <http://tass.com/defense/1036662>.

[25] Or, at least, as advertised at international arms expos. <https://rg.ru/2018/03/26/poiavilos-pervoe-foto-rossijskogo-dalnego-bespilotnika-orion.html>

[26] “Reconnaissance and attack drones to arrive for Russian Army from 2019,” Russian News Agency, December 18, 2018, <http://tass.com/defense/1036662>.

[27] “Russia’s heavy strike drone to make debut flight in spring,” Russian News Agency, December 19, 2018, <http://tass.com/defense/1036780>.

[28] “Появились первые фотографии тяжелого беспилотника «Охотник»,” Izvestia, January 24, 2019, <https://iz.ru/837713/2019-01-24/poiavilis-pervye-fotografii-tiazhelogo-bespilotnika-okhotnik>.

[29] “Russia to furnish advanced Korsar drones with electronic warfare systems,” Russian News Agency, May 8, 2018, <http://tass.com/defense/1003325>.

[30] Viktor Sokirko, “Беспилотник «Корсар»: в чем главные достоинства уникальной новинки,” Zvezda, May 28, 2018, <https://tvzvezda.ru/news/opk/content/201805281031-psxq.htm>.

[31] Kelsey D. Atherton, “Russia’s Carnivora is designed for a drone-eat-drone world,” CHISR Net, December 13, 2018, <https://www.c4isrnet.com/unmanned/2018/12/14/russias-carnivora-is-designed-for-a-drone-eat-drone-world/>.

[32] Ibid.

[33] Samuel Bendett, “Is Russia Building an Army of Robots?” The National Interest, March 19, 2018, <https://nationalinterest.org/blog/the-buzz/russia-building-army-robots-24969 >.

[34] Sam Bendett, “81. “Maddest” Guest Blogger!” Mad Scientists Laboratory blog, September 10, 2018, <https://madsciblog.tradoc.army.mil/tag/sam-bendett/ >.

[35] “Боевой робот «Уран-9» поступил на вооружение российской армии,” Izvestia, January 24, 2019, <https://iz.ru/837551/2019-01-24/boevoi-robot-uran-9-postupil-na-vooruzhenie-rossiiskoi-armii>.

[36] Dave Majumdar, “Russia Tests New "Unmanned Ground Combat Vehicle" in Near Combat Conditions,” The National Interest, January 21, 2018, <https://nationalinterest.org/blog/the-buzz/russia-tests-new-unmanned-ground-combat-vehicle-near-combat-24164>.

[37] “Russia to accept advanced robotic mine-clearing vehicles in 2018,” Russian News Agency, May 22, 2018, <http://tass.com/defense/1005519>.

[38] Svetlana Tsygankova, “В России разработают 17 подводных беспилотных аппаратов,” Rossiyskaya Gazeta, November 1, 2018, <https://rg.ru/2018/11/01/smi-v-rossii-razrabotaiut-17-bespilotnyh-podvodnyh-apparatov.html>.

[39] Timur Alimov, “Как устроена применяемая в Сирии первая в РФ подлодка-робот,” Rossiyskaya Gazeta, September 8, 2018, <https://rg.ru/2017/09/08/kak-ustroena-primeniaemaia-v-sirii-pervaia-v-rf-podlodka-robot.html>.

[40] “ВМФ РФ получил первую партию подводных аппаратов "Гавиа",” RIA Novosti, August 20, 2013, <https://ria.ru/20130820/957476811.html>.

[41] Oceanos, Press Release, March 7, 2018, “Арктика - место для роботов,” <https://oceanos.ru/news/228>.

[42] “Russian Navy to put over 30 Poseidon strategic underwater drones on combat duty – source,” Russian News Agency, January 12, 2019, <http://tass.com/defense/1039603>.

[43] “Putin says genetics, artificial intelligence most interesting areas of research for him,” Russian News Agency, December 13, 2018, <http://tass.com/politics/1035865>.

[44] Advanced Research Foundation (Фонд перспективных исследований - ФПИ), “Искусственный интеллект. Когнитивные технологии,” Accessed November-December 2018, <http://fpi.gov.ru/activities/areas/information/iskusstvenniy_intellekt_kognitivnie_tehnologii>.

[45] “2018 ARF budget will remain steady,” RIA Novosti, July 6, 2016, https://ria.ru/20160706/1459588542.html (accessed December 7, 2018).

[46] “ARF proposed AI development standards to the MOD” (ФПИ предложил Минобороны стандарты для искусственного интеллекта), RIA Novosti, March 20, 2018 <https://ria.ru/technology/20180320/1516808875.html>.

[47] “Conference: Artificial Intelligence - Problems and Solutions, 2018,” (Конференция «Искусственный интеллект: проблемы и пути их решения — 2018), April 2018, <http://mil.ru/conferences/is-intellekt.htm>.

[48] “Conference: Artificial Intelligence - Problems and Solutions, 2018,” (Конференция «Искусственный интеллект: проблемы и пути их решения — 2018), April 2018, <http://mil.ru/conferences/is-intellekt.htm>.

[49] “Shoigu called on military and civilian scientists to jointly develop robots and UAVs” (Шойгу призвал военных и гражданских ученых совместно разрабатывать роботов и беспилотники), TASS.ru. March 14, 2018. <http://tass.ru/armiya-i-opk/5028777>

[50] “Conference: Artificial Intelligence - Problems and Solutions, 2018” (Конференция «Искусственный интеллект: проблемы и пути их решения — 2018), April 2018, <http://mil.ru/conferences/is-intellekt.htm>.

[51] Ibid.

[52] “The majority of MOD’s science schools are working on AI and robotics” (Большинство научных школ Минобороны работает над искусственным интеллектом и роботами), Russian News Agency, March 15, 2018, <http://tass.ru/armiya-i-opk/5034153>.

[53] Samuel Bendett, “Russia: Expect a National AI Roadmap by Midyear,” Defense One, January 8, 2019, <https://www.defenseone.com/technology/2019/01/russia-expect-national-ai-roadmap-midyear/154015/>.

[54] Samuel Bendett, “Putin Orders Up a National AI Strategy,” Defense One, January 31, 2019. https://www.defenseone.com/technology/2019/01/putin-orders-national-ai-strategy/154555/?oref=d-river

[55] Ministry of Defense of the Russian Federation, “MOD’s innovation technolpolis will appear in Anapa,” (Инновационный технополис Минобороны РФ появится в Анапе,), Defence.ru, February 22, 2018, <https://defence.ru/article/innovacionnii-tekhnopolis-minoboroni-rf-poyavitsya-v-anape/>.

[56] “Conference: Artificial Intelligence - Problems and Solutions, 2018,” (Конференция «Искусственный интеллект: проблемы и пути их решения — 2018), April 2018, <http://mil.ru/conferences/is-intellekt.htm>.

[57] “First regional representatives from Siberia, Volga region and Ural are selected for the ERA technopolis,” (Первые представители регионов Сибири, Поволжья и Урала отобраны для технополиса "Эра,"), Russian News Agency, June 27, 2018, <http://tass.ru/armiya-i-opk/5327799>.

[58] Konstantin Tigrov. “В Минобороны рассказали о применении искусственного интеллекта в ВС РФ,” Zvezda, March 15, 2018, <https://tvzvezda.ru/news/forces/content/201803151914-bcyl.htm>.

[59] “AI development is necessary for successful cyber wars,” (Развитие искусственного интеллекта необходимо для успешного ведения кибервойн), March 14, 2018,
<https://function.mil.ru/news_page/person/more.htm?id=12166660@egNews>.

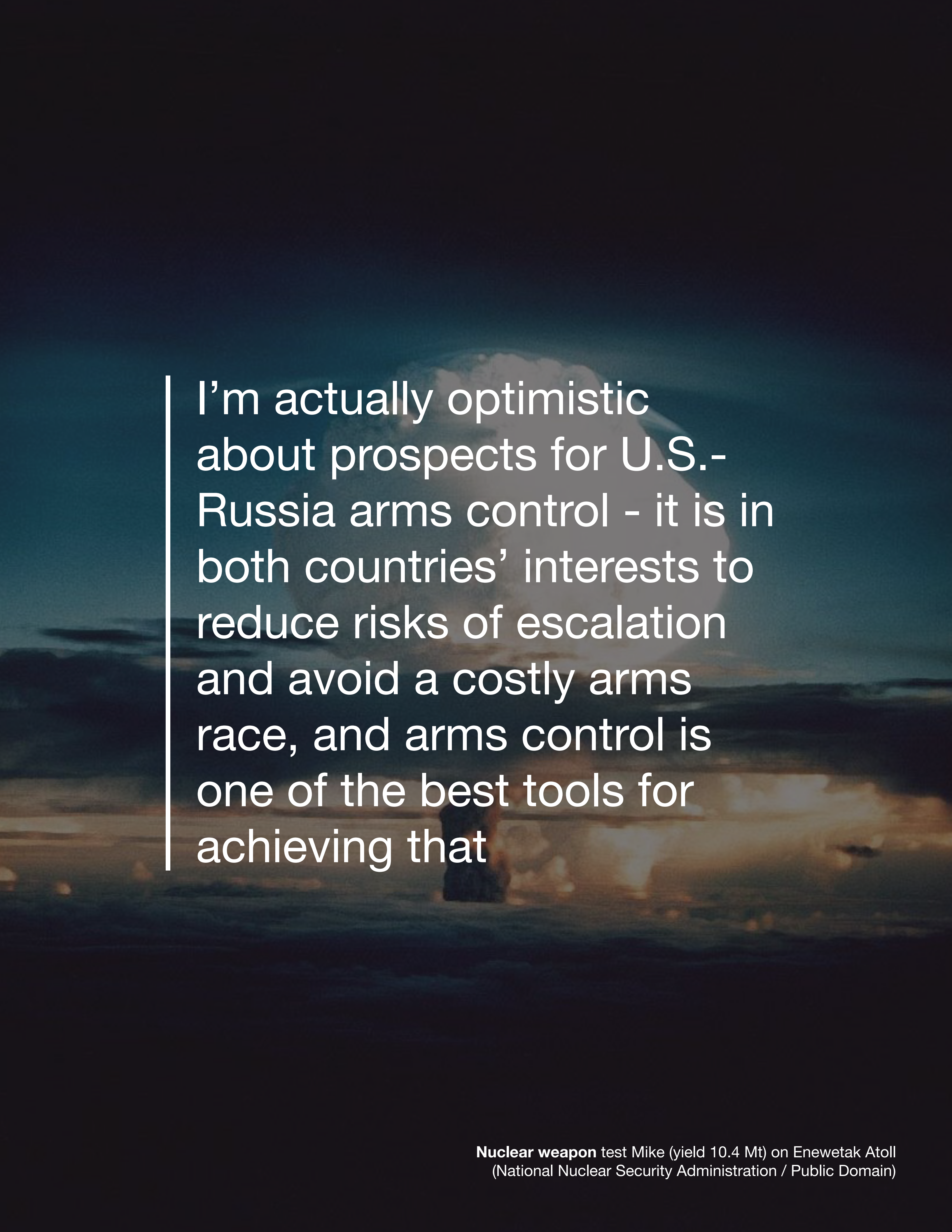
[60] Dan Robitzski, “Google Ditches Department of Defense, Updates Its Code of Ethics,” Futurism, June 1, 2018, <https://futurism.com/maven-google-military-tech>.

[61] “Управление (строительства и развития системы применения беспилотных летательных аппаратов) ГШ ВС РФ,” Ministry of Defense of the Russian Federation website, <https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11864@egOrganization> (accessed February 4, 2019).

[62] “Главное управление научно-исследовательской деятельности и технологического сопровождения передовых технологий (инновационных исследований) Министерства обороны Российской Федерации,” Ministry of Defense of the Russian Federation website, <https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11376@egOrganization> (accessed February 4, 2019).

## Samuel Bendett

Samuel Bendett is a Researcher at the CNA and a Fellow in Russia Studies at the American Foreign Policy Council. The views expressed here are his own.



> I’m actually optimistic about prospects for U.S.-Russia arms control - it is in both countries’ interests to reduce risks of escalation and avoid a costly arms race, and arms control is one of the best tools for achieving that

**Nuclear weapon** test Mike (yield 10.4 Mt) on Enewetak Atoll
(National Nuclear Security Administration / Public Domain)

# Challenges Technologies Pose to U.S.-Russia Arms Control

## A Conversation with Dr. Heather Williams

Interviewed by FSR Staff

**Fletcher Security Review:** Could you describe your current work on U.S.-Russia arms control?

**Heather Williams:** For the past two years, I have participated in Track 1.5 and Track 2 dialogues with Russia, specifically on arms control. As you can imagine, these have largely been dominated by disputes around the INF Treaty. The dialogues can be frustrating due to a tendency to "shame and blame," but they are also a great opportunity to hear the Russian perspective and try to foster dialogue. I'm encouraged by these dialogues as we often identify areas of misunderstanding and miscommunication, and because they typically include a next generation component. I'm hopeful these relationships will carry over and lay the groundwork for dialogue for decades to come. At the same time, the dialogues are very difficult at present and it is impossible to ignore the feelings of distrust on both sides.

Additionally, I lead studies on the future of arms control with a focus on potential for U.S.-Russia strategic bilateral arms control. Over the long-term, I'm actually optimistic about prospects for U.S.-Russia arms control - it is in both countries' interests to reduce risks of escalation and avoid a costly arms race, and arms control is one of the best tools for achieving that. However, arms control of the future is likely to look different from arms control of the past. There are limited prospects for the U.S. Senate ratifying another treaty, especially in light of Russia's violations of the INF Treaty. Arms control might no longer be bilateral strategic legally-binding treaties, but rather asymmetric exchanges and confidence-building measures. In the short-term, however, this is a difficult time for arms control as both the Unit-

**Soviet Union General Secretary** Gorbachev (left) and United States President Reagan (right) signing the INF Treaty (White House Photographic Office / Public Domain) ed States and Russia feel cheated and like the other side can't be trusted.

**FSR:** How has social media impacted conflict escalation, particularly between the United States and Russia? Do you think it will escalate tensions further, or become less motivating?

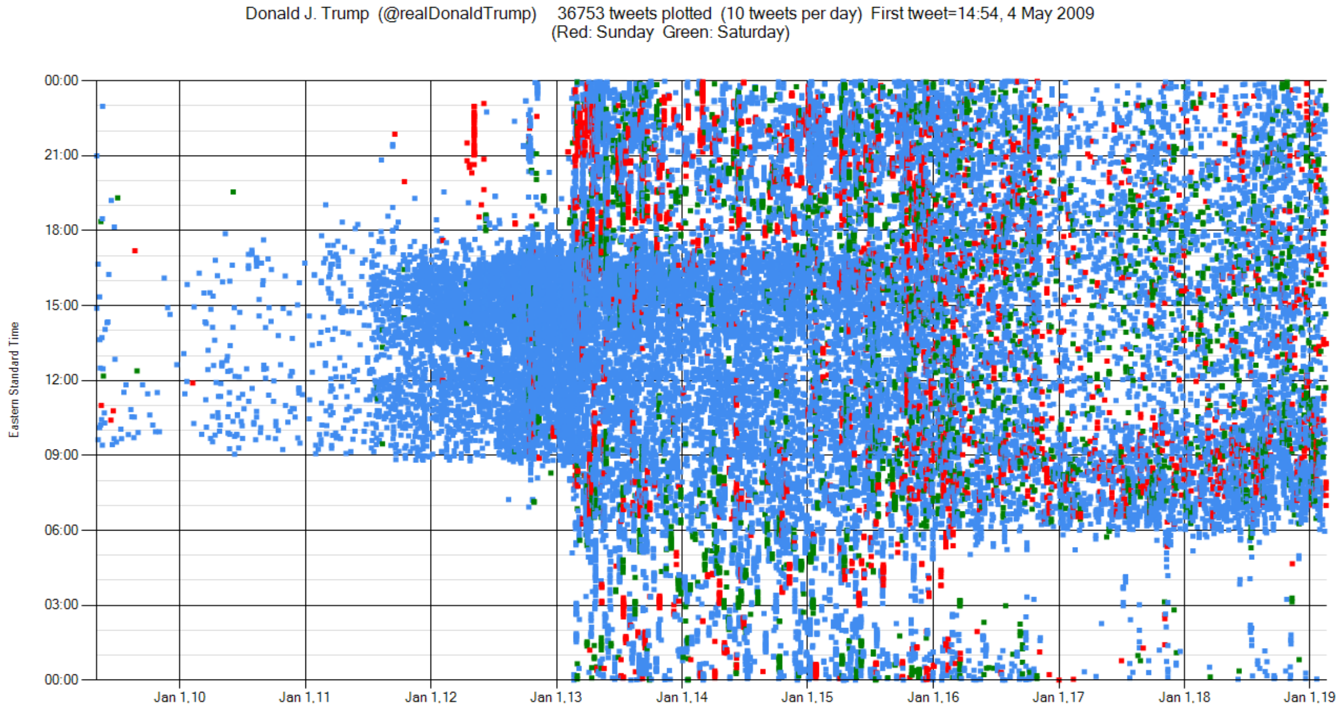
**HW:** Social media has the potential to increase the risks of misperception leading to conflict escalation. But there is still a lot about social media, and other potentially disruptive technologies, that we don't understand. Are tweets interpreted the same way as more traditional forms of signaling? What makes a tweet credible? Ultimately, I don't think a tweet can start a war, but rather the underlying geopolitical context (and contests) could create a highly volatile environment in which all signals are likely to be misinterpreted. Especially given some domestic trends in the both the United States and Russia, these signals might be represented as particularly threatening and cause for pre-emption or escalation. Another concern with social media signals is that we don't know what is real and what is bluster. If a government is trying to signal something, I doubt they would use Twitter to do so, and for the most part, social media falls into the "bluster" category. But if someone ever did try to use it to send genuine signals, we would probably miss it. Again, the geopolitical context in which this happens is extremely important.

**FSR:** In your perspective, are we likely to see an increase in other types of weaponry—conventional, AI, cyber—before any progress is made in nuclear disarmament?

**HW:** Yes, we are already seeing it. These emerging technologies add to the complexity of strategic stability, threatening arms races of crisis escalation, depending on how they are used. Countries with a conventional or nuclear disadvantage may try to exploit these technologies asymmetrically to strengthen their deterrence or gain a strategic advantage. At the same time, these technologies could reduce reliance on nuclear weapons. Ultimately, we don't yet fully understand whether or not they will have a stabilizing or de-stabilizing effect.

**FSR:** What do you see as the largest obstacles to disarmament? Are they changing?

**HW:** The return to great power competition presents a significant challenge for nuclear reductions and disarmament. Ultimately countries rely on nuclear deterrence or extended nuclear deterrence because they feel it is



**Twitter activity** of Donald Trump from his first tweet in May 2009 to May 2018. Data source from @realDonaldTrump (Phoenix7777 / CC BY-SA 4.0)

**President of Russia** Dmitry Medvedev (left) and President of the United States Barack Obama (right) discuss New START (The Russian Presidential Press and Information Office / CC BY 4.0)

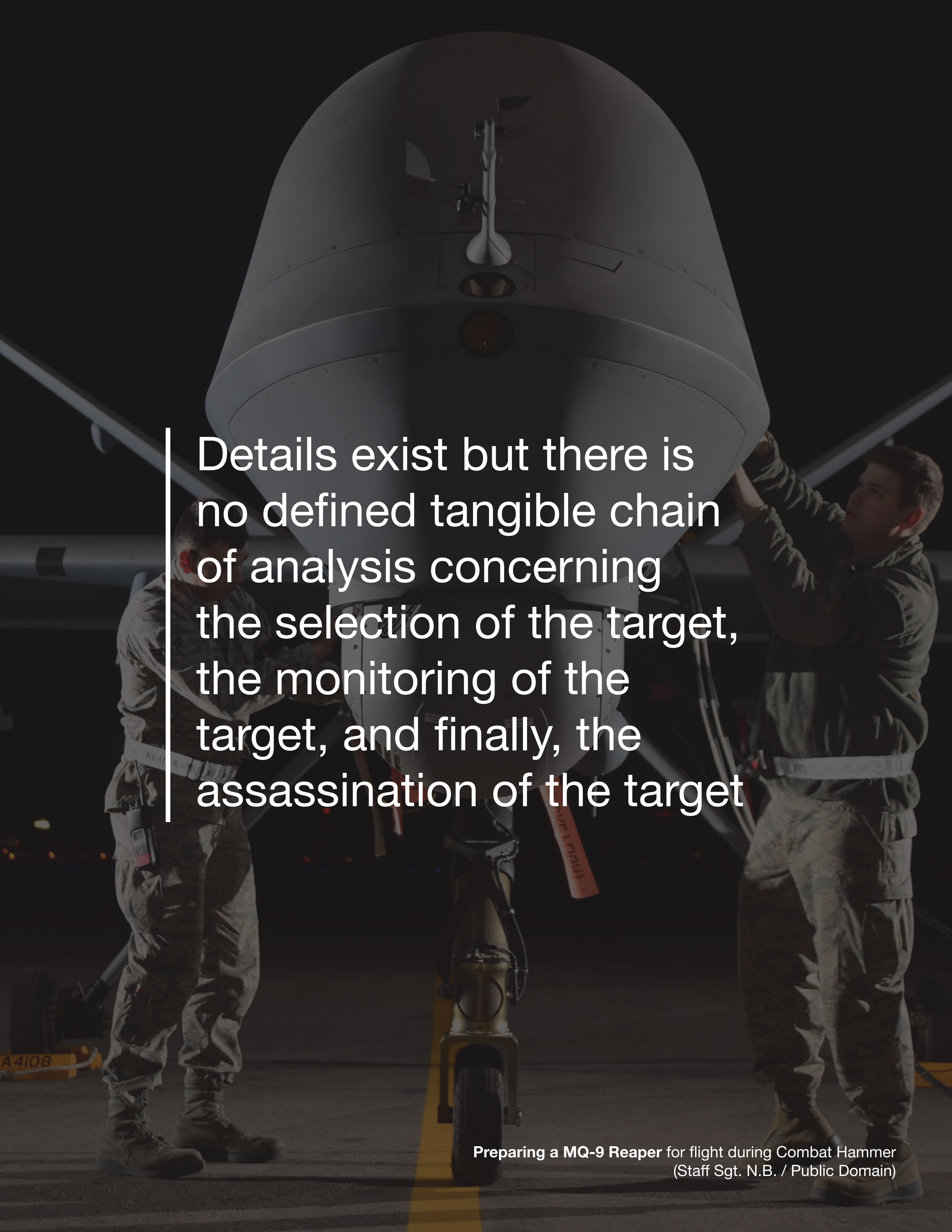
essential to their security and deterring nuclear or other existential threats. President Barack Obama's statements about pursuing the "peace and security of a world without nuclear weapons" were made during a very different era of U.S.-Russia relations. Russian aggression in Ukraine and pursuit of new nuclear capabilities, such as intermediate-range cruise missiles, has confirmed the importance of nuclear deterrence for many European states. Despite this, however, I do not think nuclear disarmament is impossible - rather, both the United States and Russia have a shared interest in reducing the risks of nuclear use, which includes arms control and arms reductions.

**FSR:** Do you think nuclear disarmament is possible in our lifetime? If so, how might it come about and how long might the process be?

**HW:** Probably not in my lifetime. But the pursuit of that goal is a worthy objective as long as it does not undermine strategic stability, increase the likelihood of conflict, or jeopardize America's commitment to its allies. It's worth recalling that arms control does not equal disarmament. Arms control is actually a tool for security and defense policy to gain insight into an adversary's arsenal and reduce risks. No matter how bad U.S.-Russia relations are, I believe neither wants a conflict to escalate to nuclear use (allegations that Russia has a doctrine of "escalate-to-deescalate" misrepresent its strategy). This fundamental and shared interest should be the foundation going forward and takes two forms. On the one hand, it requires a strong deterrent to signal commitment and prevent escalation. And on the other hand, it requires a willingness to engage in dialogue. Right now, that balance is about 90:10 and both sides are understandably distrustful because of treaty violations and withdrawals. But history shows the balance can swing the other way either due to a change in personalities, a "close call", or given enough time when geopolitics improve.

## Dr. Heather Williams

Dr. Heather Williams is a lecturer in the Defence Studies Department and Centre for Science and Security Studies at King's College London. She also does research for the Institute for Defense Analyses on Strategy, Forces, and Resources, and previously was a Research Fellow at Chatham House. Williams received her doctorate from King's College London for her dissertation on U.S.-Russia arms control from 1968-2010.



> Details exist but there is no defined tangible chain of analysis concerning the selection of the target, the monitoring of the target, and finally, the assassination of the target

**Preparing a MQ-9 Reaper** for flight during Combat Hammer
(Staff Sgt. N.B. / Public Domain)

# The Intelligence Cycle of Targeted Killing in the United States

Dr. Christine Sixta Rinehart

The United States has been using Remotely Piloted Aircraft (RPA) to assassinate terrorist targets since its first RPA strike on November 3, 2002, when a U.S. Predator fired a hellfire missile at a car traveling through the Mar'ib province of Yemen. The intelligence cycle of this targeted killing process is murky at best, and the policy has changed throughout the successive administrations of U.S. presidents. Details exist but there is no defined tangible chain of analysis concerning the selection of the target, the monitoring of the target, and finally, the assassination of the target. This paper attempts to elucidate the intelligence chain of analysis concerning American targeted killing and examine how the intelligence cycle of targeted killing varies through successive presidential administrations.

This paper will begin with a short analysis of relevant literature, although sources concerning this topic are scarce. The occurrence of targeted killings of U.S. citizens will also be explained in the literature section. The paper will continue with an elaboration of a generic intelligence cycle model, which will be used to illustrate the intelligence cycle of U.S. targeted killings using both the Reaper and the Predator RPA.[1] The paper will then address differences in the intelligence cycles and processes that have occurred between successive presidents since targeted killing first began in 2002 with President George W. Bush. Lastly, the paper will provide policy prescriptions in reference to improving targeted killing in the Middle East and Africa.

## WHAT DOES THE LITERATURE SAY?

The concept of targeted killing requires some elaboration so the reader can understand how the process works. The United States first developed its own RPAs (previously known as Unmanned Aerial Vehicles) under the Clinton administration. Originally, the RPAs were used for surveillance and reconnaissance, but, eventually, after witnessing a similar strategy used by Israel, the idea emerged that Hellfire Missiles could be strapped onto RPAs to destroy targets. RPAs have been developed by the Israelis for reconnaissance, surveillance, and targeted killing during the Intifadas. However, the Israelis were not keen on sharing the technology with the United States. U.S. companies such as Boeing and Northrop Grumman subsequently developed the U.S. RPA technology used for the surveillance and targeted killing of terrorists.

Targeted killing is defined as the pursuit and assassination of terrorists. RPAs are mostly used for reconnaissance, in addition to surveillance and assassination. The targets are found and/or hunted on a regular basis by pilots located primarily at Creech Air Force Base outside Las Vegas, Nevada, or the Air Operations Center (AOC) at al-Udeid Air Base in Qatar. Pilots and sensor operators are trained at Holloman Air Force Base in Alamogordo, New Mexico. Sensor operators help determine wind speeds and weather conditions to assist the pilots, as well as guide the Hellfire missile to the target once fired. The pilot is responsible for remotely flying the RPA. Pilots and sensor operators sit next to one another in tractor trailer storage containers, communicating constantly, as they fly RPAs located on bases across the Middle East and Africa.  The technology is located in enclosed tractor trailers like those that are used on semis to quickly move and transport the technology. Pilots can see within about ten feet of the target on a clear day, so they will most likely never see the RPAs that they are operating. All care and maintenance of the RPAs occurs at the bases in the Middle East and Africa. The RPAs are tracked and monitored by teams commonly known as the Distributed Common Ground System (DCGS), which are located all over the world.

When a target is located and the occasion is suitable for assassination, one or two Hellfire Missiles that have been strapped to an RPA are used to kill the target. There is also a GBU-12 Paveway II bomb or 500-pound bomb strapped on to the RPA. Typically, a short lapse occurs after firing due to all the integrated communication systems throughout the world that are working together. Pilots and sensor operators will usually return to the scene a few minutes after firing to ensure that the target is dead and to pursue more targets, (often called squirters) if necessary. The United States does not keep track of its own casualties  or at least casualty lists are not published and declassified for public consumption. Think tanks and publications such as *The Bureau of Investigative Journalism* and *The Long War Journal* keep track of targeted killing data independently. However, the U.S. Air Force, which has published data on Afghanistan, and U.S. presidential administrations disagree with their high numbers.

As time has progressed, U.S. presidents have come to rely on RPAs to support military and intelligence operations throughout the world, often assassinating targets as needed. President George W. Bush ordered approximately two RPA strikes per day during his presidency, and President Barack Obama ordered around ten RPA strikes per day.[2] On average, President Donald Trump has ordered less than ten RPA strikes per day, slightly less than President Obama.[3] The strikes have killed thousands of people in countries including Afghanistan, Iraq, Libya, Pakistan, Nigeria, Somalia, Syria, and Yemen in the pursuit of terrorists. Many of the casualties have been the result of "collateral damage," and countries such as Pakistan have citizenry suffering from post-traumatic stress disorder (PTSD) as a result of the constant noise of RPAs flying over their heads. On a positive note, several high-value terrorists have been assassinated, including Abdullah Haqqani and Abu Saif al-Jaziri. However, the collateral damage rates for these strikes are problematic and, as seen in Afghanistan, are at times as high as 11 civilians per targeted terrorist.[4] These rates are tricky to pinpoint, as the people who are identified as "noncombatants" by the local population may actually be lesser combatants or low-level terrorists within the organization.

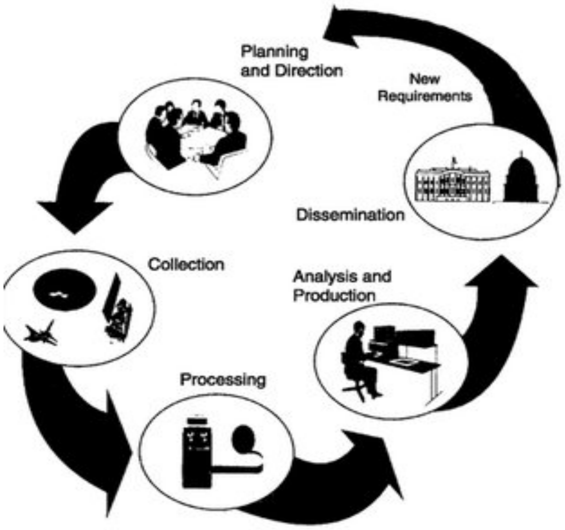
The established literature that discusses how the intelligence cycle of targeted killing works is based on anecdotal stories and personal experiences. Academic research literature does not exist. For example, the first chapter in Andrew Cockburn's book *Kill Chain* tells a detailed true story of a targeted killing attack gone awry in Afghanistan in 2010.[5] In the story, the pilot and sensor operator are given a convoy to target, which unbeknownst to them turns out to be made up of non-combatant women and children. The pilot and sensor operator are handed down the decision by higher ups who decide who and what to target. In this instance, the Air Force and intelligence agencies do not fair favorably. As illuminated by Cockburn's anecdote, the process of targeted killing appears to be quite haphazard and possibly criminal due to the various mistakes and lapses in judgement that occur. Cockburn asserts that Air Force personnel fire the Hellfire missiles just to kill *some* of the enemy. There is very little oversight over the pilot and sensor operator in this story.

In other books, such as *Predator: The remote-control air war over Iraq and Afghanistan: a pilot's story,* Lt. Colonel Matt J. Martin talks about his experiences as a RPA pilot.[6] As made evident in his book, Martin is given a significant amount of leeway as to which people should be targeted. Often, Martin would follow his assigned target for days before striking. He states: "My job was to find targets, al-Zarqawi if I were lucky. I was a patient, silent hunter. I was armed."[7] Other times, Martin would find something interesting, start following the target, and would then kill if it was a terrorist suspect.  Most likely, Martin was working under President W. Bush. In fact, one could argue that pilots and sensor operators are given unrestricted authority as to whom to target. Although the president and his administration have a wish list, in many instances the everyday targeting could be delegated to Air Force personnel. However, after numerous interviews with Creech Air Base personnel, it was affirmed that pilots and sensor operators never pick a target, nor do they have any authority over who is targeted.[8] This decision is made by Air Operations Center administration or even higher up the chain of command.

## THE INTELLIGENCE CYCLE

There are many models of the intelligence cycle. For the purpose of simplicity, we will use the basic intelligence cycle on the CIA's website, which has five stages. This process is illustrated in *Figure 1: The Intelligence Cycle*. The first stage is planning and direction. In this stage, the consumer will ask for the intelligence that they need. The consumer may be anyone from the president of the United States to leadership in the CIA or FBI.  Military intelligence or the Department of Defense may also be a consumer. In the next step, entitled "collection," information will be gathered from numerous sources both covertly and overtly by military intelligence, the CIA, FBI, or Department of Homeland Security. In the third stage, the data will be processed and put into an intelligence report. The fourth stage includes analysis and production, where the effects of the information are analyzed. For example, it will be determined what is occurring, why certain situations are occurring, what could possibly occur next, and lastly, how it affects the actor that asked for the intelligence or other actors. In the last step of the intelligence cycle, the information will be disseminated to the original requesting party, in addition to interested third parties that may need to know the intelligence.[9]

*Figure 1: The Intelligence Cycle*[10]



Although this is a basic model, veteran Air Force officer Arthur S. Hulnick found numerous problems with the model that should be acknowledged. The first problem with this model is that policymakers usually do not ask for intelligence. Rather, intelligence personnel typically predict the needs of policymakers and take the initiative to find the information that is deemed necessary. In the next step of the intelligence cycle process, gaps of information will be filled once the process is underway. Some information will take months to find and the process is not neat and tidy. In fact, the process may occur in a roundabout way where parties communicate back and forth concerning information. Hulnick states that the real drivers of the intelligence cycle are intelligence managers who are usually operating parallel to policymakers. In many instances, information sharing does not occur between intelligence agencies and policymakers due to "information restriction, psychological barriers, fear of compromising sources, and security concerns."[11] Intelligence personnel will often hold back the most pertinent and necessary information until the generic reports have been delivered to senior policy officials. For the most part, the purpose of withholding information is to highlight certain personnel or to score brown-nosing points with officials. Hulnick points out that these problems occur when the intelligence cycle confronts the real world.

The targeted-killing intelligence cycle does not necessarily follow this model either, but it does give us somewhere to start. Like Hulnick states: "The intelligence cycle is a flawed vision, and thus poor theory. One need only ask those who have toiled in the fields of intelligence."[12] In the targeted-killing intelligence model, the planning and direction stage can be initiated by numerous actors. These actors may include the president, the president's administration, the CIA, the FBI, top military personnel, or on-the-ground Air Force personnel. There are two kinds of targeted killing strikes—personality and signature strikes—although policymakers, not the U.S. Air Force, use this language. Personality strikes are targeted attacks on a person who has been identified as a terrorist leader. These strikes are usually ordered by the president or top officials, depending on the administration in power. A signature strike targets a militant who might be unknown but who has been determined through patterns of life and surveillance to be a part of a terrorist organization. In the case of signature strikes, Air Force personnel are often gathering information, analyzing it, and then making decisions, therefore deciding and carrying out stages two through five. Personality strikes were initiated by President Bush in Afghanistan. The "Terror Tuesday" meetings, described in detail below, that President Obama controlled were predominately organized for personality strikes. It is likely that President Obama's administration perfected, if not created, the signature strike.

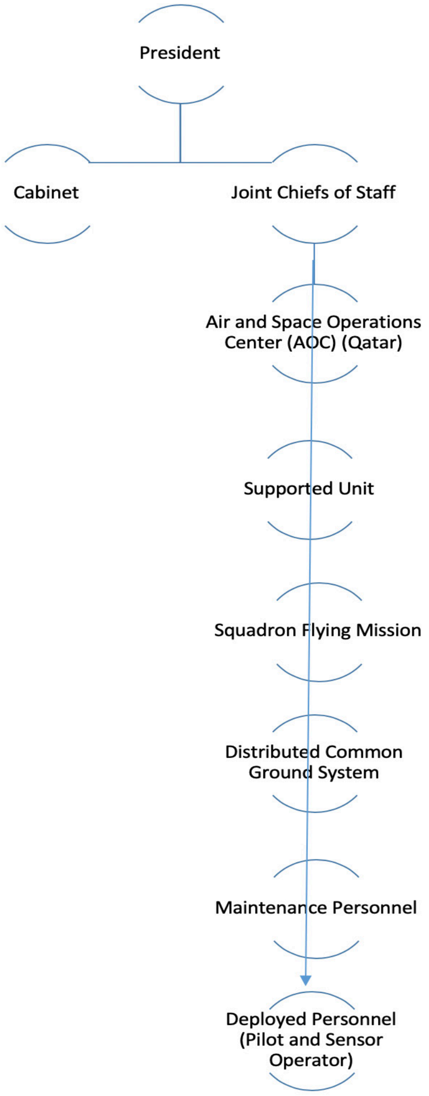
Personality strikes are usually determined by intelligence collected from the CIA and were initiated by President Bush. In carrying out a personality strike, the Special Operations Command (SOCOM) first familiarizes Special Forces with a particular geographical area. The Department of Defense's Joint Special Operations Command (JSOC) then plans RPA strikes in conjunction with the Air Force and SOCOM. SOCOM is the parent organization of JSOC, whose budget is entirely classified. Personality strikes under the Bush and Obama administrations were strictly controlled by the president and his top aides. Ultimately, however, the president and his administration made the decision as to who was to be assassinated. Under President Trump, the choice of targets has been delegated to high-ranking intelligence and military personnel. These differences between administrations will be discussed in the next section concerning the styles of various administrations. The targets may be found or chosen by numerous people along the way, depending on the strike style. That being said, it is not unlikely for pilots or sensor operators to begin following a person of interest and to then target a person once their value is assessed in signature strikes, but the AOC will make this decision. The CIA, FBI, and other intelligence agencies may also request that the Air Force look for certain people that are suspected to be within the immediate area.

Once a target is found, permission may be granted by the president and his administration, or there may have been an existing order for that person the entire time. The existing orders frequently refer to kill lists. In carrying out the strike, sensor operators and pilots must abide by the laws of war. For example, places of worship cannot be targeted and civilians should not be harmed. While there is extreme caution to prevent civilian casualties, collateral damage may occur.

As a side note, numerous sources have published reports about PTSD among Air Force RPA pilots and sensor operators, stating that the numbers are extremely high.[13] However, after the author spent a week at Creech Air Force Base, it was found that this information simply is not true. According to Colonel Julian Cheater and other Air Force personnel, the PTSD rate is around three-to-five percent, which is not significantly different from the U.S. population as a whole. In fact, the Air Force has had to include signing bonuses up to USD 175,000 for a five-year contract or USD 35,000 for each additional year of service as a result of a shortage of pilots and sensor operators, not PTSD.[14]

The following figure (*Figure 2: The Intelligence Cycle of Targeted Killing: A Preliminary Creation*) is a basic diagram of the intelligence cycle of targeted killing in the Air Force. It has more detail at the lower end of the cycle than the administrative side above AOC. However, with time and more research, this other side of the process will be furthered elaborated on. It is known that the order for the target comes from higher up the chain than the AOC. This may be the president, his staff, the Joints Chiefs of Staff, the CIA, the FBI, the Department of Homeland Security, or military intelligence. A Judge Advocate General (JAG) next approves all strikes at the AOC in Qatar.[15] The order is then given to the AOC. The AOC finds the proper supported unit, which may be RPA or a jet such as an F-16. The proper squadron is located and the DCGS, which controls communication between the various components throughout the world, is contacted. Most likely, the RPA maintenance on the ground in Qatar is the primary contact in this step of the DCGS. Lastly, maintenance personnel and the deployed personnel are given notice before the mission occurs. The RPA takes off from the base, flown by pilots and sensor operators at AOC, and is then taken over mid-air by pilots at Creech. It takes approximately seventy-two hours from the time that AOC is alerted to the assassination of the target.[16] The next section of the paper will look at the targeted killing cycle of intelligence under successive presidents.

*Figure 2: The Intelligence Cycle of Targeted Killing - A Preliminary Creation*


President
Cabinet
Joint Chiefs of Staff
Air and Space Operations Center (AOC) (Qatar)
Supported Unit
Squadron Flying Mission
Distributed Common Ground System
Maintenance Personnel
Deployed Personnel (Pilot and Sensor Operator)

**United States President** George W. Bush speaks at the Pentagon Memorial dedication ceremony (Cherie Cullen / Public Domain)

## TARGETED KILLING UNDER PRESIDENT GEORGE W. BUSH

Targeted killing pursued by an American president against his enemies is not a unique occurrence. Although the Hague Convention of 1907 outlawed the assassination of foreign leaders and the 1949 Geneva Convention followed suit, discrepancies between laws applied during peacetime and wartime have allowed presidents to subjectively pursue assassination. As an example, numerous U.S. presidents gave the order to assassinate Fidel Castro but failed. According to Castro's former secret-service chief, it is estimated that Castro received a total of 634 attempts on his life.[17] The CIA was responsible for many of those assassination attempts, including bizarre strategies such as an exploding cigar or exploding underwater seashell.[18] From Eisenhower to Clinton, every president at least tried to get rid of Castro, assassinate him, or both.[19] American presidents also played a role in the assassination attempts against Adolf Hitler. The Cold War contained a flurry of eradication attempts against foreign leaders. At one point, it became so bad that Congress passed the War Powers Resolution Act in 1973 trying to curb the war powers of the presidency and the office's power in general, although the act has had little success. It has also been illegal for a president to assassinate any enemy since 1976 when President Gerald Ford passed an executive order outlawing the practice. The culmination of the Iran-Contra scandal led to the final reigning in of the CIA and President Ronald Reagan. However, the CIA has almost returned to its previous levels of power, targeting terrorists with the acquiescence of the president, including targeting and killing several American citizens with RPAs without any due process.

President Bush played a major role in the rejuvenation of the powers of the CIA and assassination when Congress passed his Authorization for the Use of Military Force (AUMF) in 2001, in an effort to pursue all the attackers responsible for the September 11 attacks. The AUMF empowered the president "to use all necessary and appropriate force" in pursuit of those responsible for the terrorist attacks. Under the AUMF, President Bush began authorizing targeted killing in Yemen in 2002. Bush, in comparison to President Obama, was much less trigger happy when it came to targeted killing. He allowed the CIA to conduct approximately fifty-one RPA strikes, particularly in Pakistan (although he also targeted Afghanistan and Yemen), where he had the agreement of President Musharraf to conduct the strikes. Fewer than 600 people were killed as a result of RPA strikes under the Bush administration.[20] Under President Bush, the CIA would instruct the Air Force on where to find and kill targets. President Bush had given his consent to the CIA to find and kill dangerous terrorists, mostly al-Qaeda members, but he did not play a large role in the day-to-day decision making. After allowing the United States to use its airspace, Pakistan would either take credit under its Inter-Services Intelligence (ISI) or remain silent about the strikes. Problematically, things were falling from the sky on a regular basis, so Pakistani president Pervez Musharraf found it difficult to keep up the ruse.

## TARGETED KILLING UNDER PRESIDENT BARACK H. OBAMA

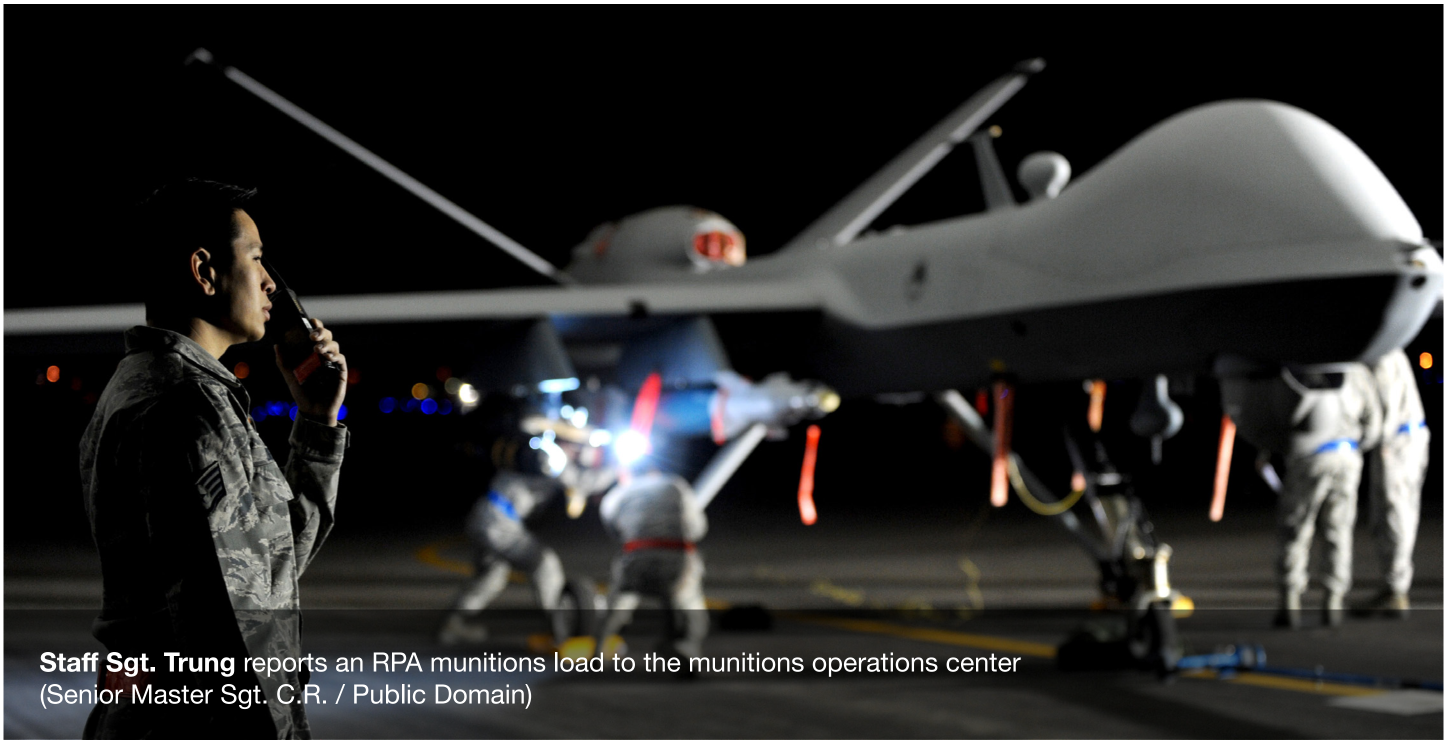
While President Obama criticized President Bush for being too aggressive on many aspects of counterterrorism, when it came to targeted killings, President Obama was much more aggressive than President Bush and used RPAs to a much greater extent to conduct targeted killings. He stated: “The Bush administration has not acted aggressively enough to go after al-Qaeda’s leadership. I would be clear that if Pakistan cannot or will not take out al-Qaeda leadership when we have actionable intelligence about their whereabouts, we will act to protect the American people. There can be no safe haven for al-Qaeda terrorists who killed thousands of Americans and threaten our homeland today.”[21]

Three days into his presidency, President Obama ordered his first RPA strikes in Pakistan. President Obama expanded the location of targeted killing throughout the Middle East and Africa by adding Libya, Nigeria, Iraq, Syria, and Somalia to the already targeted Afghanistan, Pakistan, and Yemen. The daily number of strikes increased to five times what President Bush had authorized.[22]

If President Bush was a macro-manager of targeted killing, President Obama was a micro-manager when it came to the targeted killing process. Known as the somewhat mythical “Terror Tuesdays,” pertinent Obama administration officials and high-ranking military officials would sit around a table in the White House Situation Room and study the faces of numerous terrorists. This information was presented in a condensed format called baseball cards. Using the information on the baseball cards, President Obama took around fifty-eight days to sign off on a target—forces would then have sixty days to carry out a strike against the target.[23] President Obama would study the set of biographies given to him, becoming the preeminent decision maker in who would be killed. He would even get interrupted during family time to make a decision to kill a target. Most likely, these interruptions only occurred in a sticky situation where there might be civilian deaths involved. These “Terror Tuesday” meetings formed the kill lists for personality strikes. These people were also placed on no-fly and selectee lists. There were almost 1 million people on this list, including over 5,000 Americans, during Obama’s presidency.[24]

For President Obama, there was a two-part process of an approval for an RPA strike.  JSOC Task Force 48-4 would cultivate a case for the person alongside other intelligence agencies to develop and authorize a target. The authorization and action would ultimately be given to the president. JSOC would begin by creating a case and then would pass the target on to the command center in the area, then the Joint Chiefs of Staff, and then to the Secretary of Defense. It was then given to the Principals Committee of the National Security Council. Finally, President Obama would sign off on it.[25]

Thomas E. Donilon, President Obama’s National Security Advisor stated: “[Obama] is determined to make these decisions about how far and wide these operations will go. His view is that he is responsible for the position of the United States in the world. He’s determined to keep the tether pretty short.”[26] William M. Daley, Obama’s Chief of Staff in 2011, stated: “One guy gets knocked off and the guy’s driver who’s number twenty-one becomes [number] twenty? At what point are you just filling the bucket with numbers?”[27] President Obama was highly criticized for his "whack-a-mole” approach, careless targeting, falsified RPA casualty numbers, and high number of civilian deaths. After his promise to close Guantanamo Bay Prison in Cuba and stop the torture of detainees, President Obama’s copious use of RPA strikes appeared like a *Twilight Zone* episode to liberals. However, the American public was largely ignorant of what was going on with RPA strikes, as the media rarely researched and reported on the strikes. After President Obama authorized the killing of a U.S. citizen, Anwar al-Awlaki, with an RPA strike on September 30, 2011, and targeted his sixteen-year-old-son, Abdurahman Anwar al-Awlaki, two weeks later, he realized that the legal justification for targeted killing needed some improvement, particularly in relation to killing American citizens. President Obama worked with the Department of Justice to develop the *White Paper*, which allows the military to kill American citizens outside of the United States for suspected terrorist activity, particularly if the person is “considered” an imminent threat.[28] The press rarely covered President Obama’s use of RPA strikes or the administration’s murder of U.S. citizens. One could even argue that the *White Paper* allowed RPA strikes against U.S. citizens within the United States, although to date this has not occurred.



**Staff Sgt. Trung** reports an RPA munitions load to the munitions operations center (Senior Master Sgt. C.R. / Public Domain)

In May 2013, President Obama's aides stated that signature strikes, which first began under President Bush, would be phased out. In a speech Obama delivered in May 2013, he vowed to put the fight against terrorists on better legal footing. His administration then released a three-page paper delineating the circumstances under which RPAs could strike. Under the new policy, pilots could only hit targets when there was "near certainty" that civilians would not be injured. Unfortunately, officials never explained the criteria and the rules did not apply in "areas of active hostilities."[29] Later Iraq, Syria, and Afghanistan were all marked as "areas of active hostilities," as were some parts of Pakistan. The speech and paper lacked clear criteria and the discontinuation of signature strikes failed to occur with the appearance of ISIS in Iraq and Syria. President Obama continued using signature strikes until the end of his presidency.[30]

## TARGETED KILLING UNDER PRESIDENT DONALD TRUMP

In comparison to the Obama administration, the Trump administration has executed a similar amount of strikes, although the numbers are slightly fewer, with over nine strikes per day.[31] Concerning civilian casualties, it is still too early to make comparisons between administrations. President Trump has experienced more criticism regarding his authorization of targeted killings, possibly because he is a Republican president beset by a predominately liberal press corps and academia. In comparison, very little attention was paid to President Obama's use of RPAs by both the press and academics, and not much was published concerning the effects of targeted killing and RPA warfare. The increase in publications by a left-leaning press with a combative relationship with the president has complicated President Trump's ability to continue to pursue RPA campaigns. This political pressure partially explains why President Trump has delegated the selection of targets to subordinates in the Department of Defense.[32]

The Trump administration's Principles, Standards, and Procedures (PSP) plan was approved on September 14, 2017. Under this plan, President Trump sustained President Obama's policies by continuing to target high-value targets who are a "continuing and imminent threat" to Americans.[33] In addition, President Trump expanded the policy to include "foot-soldier jihadists with no special skills or leadership roles." Foot-soldier jihadists were targeted under President Obama but were not delineated by his administration as targets. Also, proposed RPA attacks and raids are no longer subject to high-level vetting by the Oval Office. Like the Obama administration, there is no targeting of civilians. President Trump's plan extended the "pattern of giving broader day-to-day authority to the Pentagon and the CIA—authorizing the agencies to decide when and how to conduct high-risk counterterrorism operations."[34] The CIA is also able to conduct covert RPA strikes. Under this plan, high-level approval is still needed to start conducting strikes in new countries. These strikes require "country plans" that would be reviewed annually. Under international law, the United States still needs need to obtain consent from a country's leaders to use strikes on foreign soil.

As a side note, in comparison to President Obama, President Trump is not shy about publicly stating that the United States targets terrorist families. Families were regularly killed under President Obama. From a rhetoric standpoint, President Obama was careful to say that civilians were never targeted. However, previously mentioned think-tank numbers argue that civilians were frequently targeted under the Obama administration. The value of the target was high enough to endure the political backlash from killing wives and children. President Trump, on the other hand, directly stated on the campaign trail in 2015 that the families of terrorists should be targeted at times. President Trump said on *Fox and Friends* that, "when you get these terrorists, you have to take out their families. They care about their lives, don't kid yourself. But they say they don't care about their lives. You have to take out their families."[35] Although his statement has been highly criticized, it is worth noting that male terrorists will often surround themselves with women and children so that they are less likely to be targeted. In essence, women and children are treated as human shields.

In comparison, the intelligence cycle of President Trump concerning targeted killing is quite similar to that of President Bush. Like President Bush, President Trump has delegated many of the daily decisions to subordinates. President Trump has called for high-value targets to be terminated, and the CIA has planned, collected, processed, analyzed, and disseminated the output needed for high-value targets. Moreover, President Trump does not review daily targets. It is likely that, for some targets, President Trump must give the orders, but targeted killing has been handed down to the personnel in the CIA, and the CIA relies on the Air Force to carry out the missions. Signature strikes and personality strikes are still occurring, but President Trump rarely engages in determining the kill list.

## CONCLUSION AND POLICY PRESCRIPTIONS

In conclusion, RPA strikes have recently been handed to agencies within the Department of Defense by the Trump administration. The policies among Presidents Bush, Obama, and Trump have ebbed and flowed depending on who is in power. However, RPA strikes are still occurring, and the numbers are relatively consistent between Presidents Obama and Trump, although President's Trump's numbers are slightly lower. The intelligence cycle varies depending on whether the strike is a signature strike or personality strike. The CIA plays a large role in gathering information for personality strikes although they also participate in signature strikes. In signature strikes, the Air Force and military intelligence are primarily responsible for gathering intelligence and analyzing it. However, more research needs to be done to pinpoint the exact process, particularly above the AOC. This paper is an attempt at an initial intelligence process concerning targeted killing. The details need to be elaborated on and pilots and sensor operators are the best people to talk to concerning the intelligence cycle of targeted killing.

From a policy prescription perspective, it has been hinted at several times in this paper that the process needs oversight and an actual protocol put into place. Currently, the president and his or her personnel have too much leeway in determining who gets killed. There needs to be more oversight instead of a handful of people acting as both judge and jury to determine death sentences for suspected terrorists. This is particularly true in regard to the numerous American citizens who have been killed without due process by both Bush and Obama.

Although extremely useful, RPA strikes should not be used unless there is a threat of imminent danger. RPA strikes are expedient when an attack is pending or a terrorist group leader is within sight. Children, families, and civilian property, on the other hand, are not threats. Legal scholars Amos Guiora and Jeffrey Brand have suggested the establishment of RPA courts to legitimize and put legal protections into the targeting process. This idea includes a court containing 24 Article III justices, 12 justices from the district courts, and 12 justices from the Court of Appeals. While Guiora and Brand's specific idea of an RPA court is too difficult and cumbersome to implement in full, there should at least be a list of predetermined criteria that is employed when deliberating about whether or not to conduct a strike. An RPA court including a smaller number of competent judges—perhaps ten or less—could be chosen and approved by the Senate to help with this process. While this targeted-killing war machine deserves high respect for its ability to kill terrorists, it should be considerably regulated and infrequently used by the U.S. government and military.[36]

[1] The Predator was phased out at the end of 2018 and the sole targeted killing RPA is the Reaper.

[2] Christine Sixta Rinehart, *Drones and Targeted Killing in the Middle East and North Africa, An Appraisal of American Counterterrorism Policies* (Lanham, MD: Lexington Books, 2016).

[3] Christine Sixta Rinehart, "Trump's Drone Policy: The Continuation of a Legacy," *Georgetown Journal of International Affairs,* June 15, 2018, accessed July 23, 2018, https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/6/14/trumps-drone-policy-the-continuation-of-a-legacy.

[4] Christine Sixta Rinehart, *Drones and Targeted Killing in the Middle East and North Africa, An Appraisal of American Counterterrorism Policies* (Lanham, MD: Lexington Books, 2016), 117.

[5] Andrew Cockburn, *Kill Chain, The Rise of the High-Tech Assassins* (New York: Henry Holt and Company, 2015).

[6] Matt Martin, *Predator: The remote-control air war over Iraq and Afghanistan: A pilot's story* (Minneapolis: Zenith Press, 2010).

[7] Matt Martin, *Predator: The remote-control air war over Iraq and Afghanistan: A pilot's story* (Minneapolis: Zenith Press, 2010), 37.

[8] Colonel Julian Cheater, Interview by Author, Creech Air Force Base, November 29, 2018.

[9] The Central Intelligence Agency, "Kid's Zone," *The Central Intelligence Agency*, March 23, 2013, accessed July 23, 2018, https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html

[10] As cited in Loch K. Johnson and James J. Wirtz, "Introduction" in *Intelligence: The Secret World of Spies, An Anthology*, ed. Loch K. Johnson and James J. Wirtz, 4th Ed (New York: Oxford University Press, 2015), 73.

[11] Arthur S. Hulnick, "The Intelligence Cycle" in *Intelligence: The Secret World of Spies, An Anthology*, ed. Loch K. Johnson and James J. Wirtz, 4th Ed (New York: Oxford University Press, 2015), 82.

[12] Arthur S. Hulnick, "The Intelligence Cycle" in *Intelligence: The Secret World of Spies, An Anthology*, ed. Loch K. Johnson and James J. Wirtz, 4th Ed (New York: Oxford University Press, 2015), 92.

[13] Sarah McCammon, "The Warfare May be Remote but the Trauma is Real," *National Public Radio*, April 24, 2017, accessed July 23, 2018, https://www.npr.org/2017/04/24/525413427/for-drone-pilots-warfare-may-be-remote-but-the-trauma-is-real.

[14] Stephen Losey, "Air Force offers bonuses up to $175,000 for drone pilots," *Air Force Times*, October 24, 2016, accessed July 23, 2018, https://www.airforcetimes.com/news/your-air-force/2016/10/24/air-force-offers-bonuses-up-to-175000-for-drone-pilots/.

[15] *Figure 2: The Intelligence Cycle of Targeted Killing: A Preliminary Creation*

[16] Captain OL, Interview by Author, Creech Air Force Base, November 26, 2018.

[17] Alexander Smith, "Assassination Attempts," NBC News, November 28, 2016, accessed August 1, 2018, https://www.nbcnews.com/storyline/fidel-castros-death/fidel-castro-cia-s-7-most-bizarre-assassination-attempts-n688951.

[18] Alexander Smith, "Assassination Attempts," NBC News, November 28, 2016, accessed August 1, 2018, https://www.nbcnews.com/storyline/fidel-castros-death/fidel-castro-cia-s-7-most-bizarre-assassination-attempts-n688951.

[19] Charlotte England, "All the US Presidents Fidel Castro outlasted, and how they dealt with the Cuban Leader," *The Independent*, November 26, 2016, accessed August 1, 2018, https://www.independent.co.uk/news/people/fidel-castro-us-presidents-outlasted-and-how-they-dealt-with-him-eisenhower-kennedy-johnson-nixon-a7440486.html.

[20] The Bureau, "The Bush Years: Pakistan Strikes 2004-2009," *The Bureau of Investigative Journalism*, 2018, accessed August 1, 2018, https://www.thebureauinvestigates.com/drone-war/data/the-bush-years-pakistan-strikes-2004-2009.

[21] Kenneth Anderson, "Targeted Killing in U.S. Counterterrorism Strategy and Law," *The Brookings Institution*, May 11, 2009, accessed August 1, 2018, https://www.brookings.edu/research/targeted-killing-in-u-s-counterterrorism-strategy-and-law/.

[22] Christine Sixta Rinehart, *Drones and Targeted Killing in the Middle East and North Africa, An Appraisal of American Counterterrorism Policies* (Lanham, MD: Lexington Books, 2016), ix.

[23] Jeremy Scahill, "The Drone Legacy," in *The Assassination Complex,* ed. Jeremy Scahill (New York: Simon & Schuster, 2016), 7.

[24] Jeremy Scahill and Ryan Devereaux, "Death and the Watchlist," in *The Assassination Complex,* ed. Jeremy Scahill (New York: Simon & Schuster, 2016).

[25] Cora Currier, "The Kill Chain," in *The Assassination Complex,* ed. Jeremy Scahill (New York: Simon & Schuster, 2016). 60.

[26] Joe Becker and Scott Shane, "Secret 'Kill List' Proves a Test of Obama's Principles and Will," *The New York Times,* May 29, 2012, accessed August 1, 2018, https://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?pagewanted=all&_r=0.

[27] Joe Becker and Scott Shane, "Secret 'Kill List' Proves a Test of Obama's Principles and Will," *The New York Times,* May 29, 2012, accessed August 1, 2018, https://www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html?pagewanted=all&_r=0.

[28] Department of Justice, "Department of Justice White Paper" *Department of Justice*, November 8, 2011, accessed August 1, 2018, https://www.documentcloud.org/documents/602342-draft-white-paper.html.

[29] Department of Justice, "Department of Justice White Paper" *Department of Justice*, November 8, 2011, accessed August 1, 2018, https://www.documentcloud.org/documents/602342-draft-white-paper.html.

[30] Dan de Luce and Paul Mcleary, "Obama's Most Dangerous Drone Tactic Is Here to Stay," *Foreign Policy*, April 5, 2016, accessed August 1, 2018, https://foreignpolicy.com/2016/04/05/obamas-most-dangerous-drone-tactic-is-here-to-stay/.

[31] Christine Sixta Rinehart, "Trump's Drone Policy: The Continuation of a Legacy," *Georgetown Journal of International Affairs*, June 14, 2018, accessed August 1, 2018, https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/6/14/trumps-drone-policy-the-continuation-of-a-legacy.

[32] Christine Sixta Rinehart, "Trump's Drone Policy: The Continuation of a Legacy," *Georgetown Journal of International Affairs*, June 14, 2018, accessed August 1, 2018, https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/6/14/trumps-drone-policy-the-continuation-of-a-legacy.

[33] Charlie Savage and Eric Schmitt, "Trump Poised to Drop Some Limits on Drone Strikes and Commando Raids," *The New York Times*, September 21, 2017, accessed August 1, 2018, https://www.nytimes.com/2017/09/21/us/politics/trump-drone-strikes-commando-raids-rules.html?_r=0.

[34] Charlie Savage and Eric Schmitt, "Trump Poised to Drop Some Limits on Drone Strikes and Commando Raids," *The New York Times*, September 21, 2017, accessed August 1, 2018, https://www.nytimes.com/2017/09/21/us/politics/trump-drone-strikes-commando-raids-rules.html?_r=0.

[35] Jesse Byrnes, "Trump on terrorists: You have to take out their families," *The Hill*, December 2, 2015, accessed August 1, 2018, http://thehill.com/blogs/ballot-box/presidential-races/261757-trump-on-terrorists-you-have-to-take-out-their-families.

[36] Christine Sixta Rinehart, "Trump's Drone Policy: The Continuation of a Legacy," *Georgetown Journal of International Affairs*, June 14, 2018, accessed August 1, 2018, https://www.georgetownjournalofinternationalaffairs.org/online-edition/2018/6/14/trumps-drone-policy-the-continuation-of-a-legacy.

## Dr. Christine Sixta Rinehart

Dr. Christine Sixta Rinehart is an Associate Professor of *Political* Science at the University of South Carolina in Palmetto College. She earned her PhD from the University of South Carolina in 2008. Her research interests include international terrorism, female terrorism, and security and counterterrorism. Her first book *Volatile Social Movements and the Origins of Terrorism: The Radicalization of Change* was published in December 2012 by Lexington Books. Her second book, *Drones and Targeted Killing in the Middle East and Africa: An Appraisal of American Counterterrorism Policies* was published by Lexington Books in December 2016. Her third book, *Sexual Jihad: The Role of Islam in Female Terrorism* will be published in spring 2019 by Lexington Books.  She can be reached at sixta@mailbox.sc.edu

> Only political intervention through mutual understanding, doctrinal prudence, and regulating the search for operational supremacy holds potential to escape the stranglehold of the action-reaction cycle

**Testing** of the Peacekeeper MIRV
(David James Paquin / Public Domain)

# Sino-Indian Nuclear Dynamics

## Taking the Global Lead

Lt. Gen. (Dr.) Prakash Menon

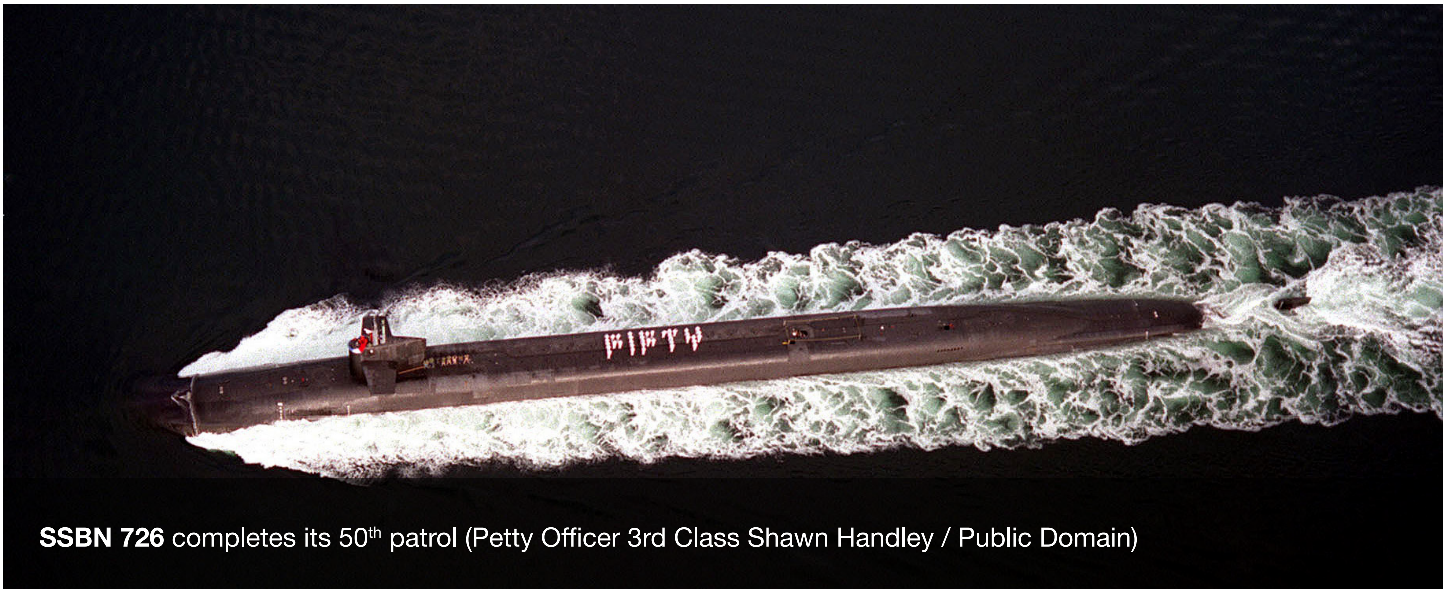
Technology often seduces potential adversaries through a promise of relief from security threats only to deceive through the inevitable action-reaction cycle. In the universe of security, technology is contestable both by technology itself and by doctrinal prescriptions and operational countermeasures. The advantage provided by new technology is mostly ephemeral in that provides the momentum for an endless cycle that is best described as chasing one's own tail. Only political intervention through mutual understanding, doctrinal prudence, and regulating the search for operational supremacy holds potential to escape the stranglehold of the action-reaction cycle. The elusive search for Ballistic Missile Defense (BMD) is a prime example. This paper seeks to interrogate the role of the technology-security dynamics in the context of the Sino-Indian nuclear weapon relationship.

The context of the Sino-Indian nuclear weapon relationship is clouded by the enhancing reach of India's missiles[1], the evolving Chinese reaction to U.S. nuclear modernization accompanied by a shift in nuclear posture, and a shared belief in the role of nuclear weapons that is signified by No First Use (NFU) doctrine. The latter point represents political intervention while the two former signify the action-reaction cycle which is primarily a product of technology. However, both China and India must contend with nuclear powers that espouse First Use. China in dealing with the United States and Russia who are quantitatively superior nuclear powers, while India deals with Pakistan whose claims of quantitative superiority are contested.

In technological terms, the rise of China and the U.S. reaction resulting in contemporary geopolitical flux at the global level has impacted the evolution of China's nuclear arsenal. The most prominent illustration of this is China's reaction to the United States' withdrawal from the Ballistic Missile Defense Treaty. Earlier China had eschewed development of BMD, but the United States' quest to create BMD has caused China to attempt to develop its own BMD system as well as systems that can overcome BMD like multiple independently targetable reentry vehicles (MIRVs) and Hyper Glide Vehicles (HGVs). Similarly, India has reacted to developments in China and Pakistan by launching an indigenous BMD development program.

The key question is whether the political embrace of the belief in the role of nuclear weapons that underpins China's and India's NFU posture restrains technological trajectory which in contemporary times is also

**Beijing, China.** DF-26 medium-range ballistic missile as seen after a military parade (IceUnshattered / CC BY-SA 4.0)



**SSBN 726** completes its 50th patrol (Petty Officer 3rd Class Shawn Handley / Public Domain)

fashioned by cyber power, synthetic biology, artificial intelligence, and robotics, inter alia. Both countries emphasize the political nature of nuclear weapons and deride its war fighting potential. Neither believe in quantitative supremacy and hold dear the notion that survivability of a few weapons is enough for deterrence. These beliefs provide an explanation of the existing size of the arsenals of both countries which indicates that quantitative parity with adversaries is not on the agenda. Though lack of resources and technological capability may provide an alternate explanation, it reflects political acceptance of sufficiency instead of reconciliation to inability.

Recent reports on China's[2] and India's[3] nuclear arsenal are revealing. Both China and India are in the process of technologically upgrading their arsenal rather than expanding their number of missiles and warheads. Both countries are replacing liquid propelled missiles with solid-fueled ones. Warhead numbers are increasing, but only marginally. Survivability enhancement through land mobile missiles and ballistic missile submarines (SSBNs) outlines the direction of growth of the arsenal. Both are increasing the range of missiles to cover the entire land mass of the larger adversary. The major difference is in China's massive increase in missiles with conventional warheads. Notably, China houses both class of missiles within a common organizational structure. India's arsenal of conventional missiles is not only separately controlled but is still in a nascent stage of development.

In both countries, nuclear weapons are de-mated with the warheads and missiles stored separately which in turn reflects the rejection of the worst-case scenario of the "bolt from the blue" attack. This is the reason why the United States and Russia continue to keep some of their arsenals at high alert levels. This will change to some extent for China and India when the SSBNs are fully operational, but it would be because of technological necessity and not because of the danger due to "bolt from the blue". More importantly, both countries continue to adhere to NFU despite pressures from within for a review. The triumph of political doctrine over technological seduction that promises to deliver solutions to nuclear deterrence is evident. But what does the adherence to NFU imply for the Sino-Indian nuclear weapon relationship?

NFU doctrine of both China and India is rooted in the belief that nuclear weapons only have the core role of deterring their own kind. Both countries believe that the notion of a successful first strike is a mirage and a product of a military imagination that is politically abstracted due to the probability of severing the link between force application and achievement of political objectives. Such a possibility exists even when the initial exchange commences with low-yield weapons that nuclear war fighting adherents believe can be contained to a tolerable level of exchange. The reality is that there is no knowing what happens after the first nuclear weapon is fired at another nuclear-armed power. Historically, nuclear powers have exercised caution during crises even if pre-crisis rhetoric was bellicose.

The major payoff from NFU is that there is no room to

**An Indian Agni-II** intermediate range ballistic missile on a road-mobile launcher (Antônio Milena/ CC BY 4.0)

hurl nuclear threats except in retaliation for nuclear use. If the most common scenario for nuclear use between India and China is consequent to a conventional war, NFU raises the bar of nuclear use. It would require more than a stretch of imagination to visualize an issue that could justify the risk of nuclear first use by either party. Admittedly, if both sides alert their weapons, there is the possibility of nuclear use through accident, misjudgment, misperception, miscommunication and the unknowable impact of what Clausewitz described as friction. The greater possibility for use would be due to China's salami-slicing tactics which would mean limited land grabs. Nuclear weapons have no role in such a scenario but could impose caution and prevent escalation.

NFU offers the feasibility of greater stability. As the contemporary world drifts into dangerous geopolitical waters, it is time that India and China work together to vaccinate other nuclear weapon powers with NFU. Fundamentally, other nuclear weapon powers must be convinced of the need to make the world safer through privileging political doctrines that reduce the probability of nuclear use and not through technological solutions in the name of strengthening deterrence. India and China are best placed to take the lead for evolving a Global No First Use (GNFU) Treaty since their nuclear dynamics do not threaten the world, as opposed to U.S.-Russia dynamics.

Complete nuclear disarmament is a laudable objective that is presently impeded by an increase in the global geopolitical rivalry. GNFU provides an interim step that could inject much-needed safety to a world that seems to once again be heading down the slippery slope of buttressing nuclear deterrence. China and India must seize this opportunity by rendering their convergence of nuclear ideology as a cooperative endeavor which could be met by privileging political prudence over deceptive technological fixes.

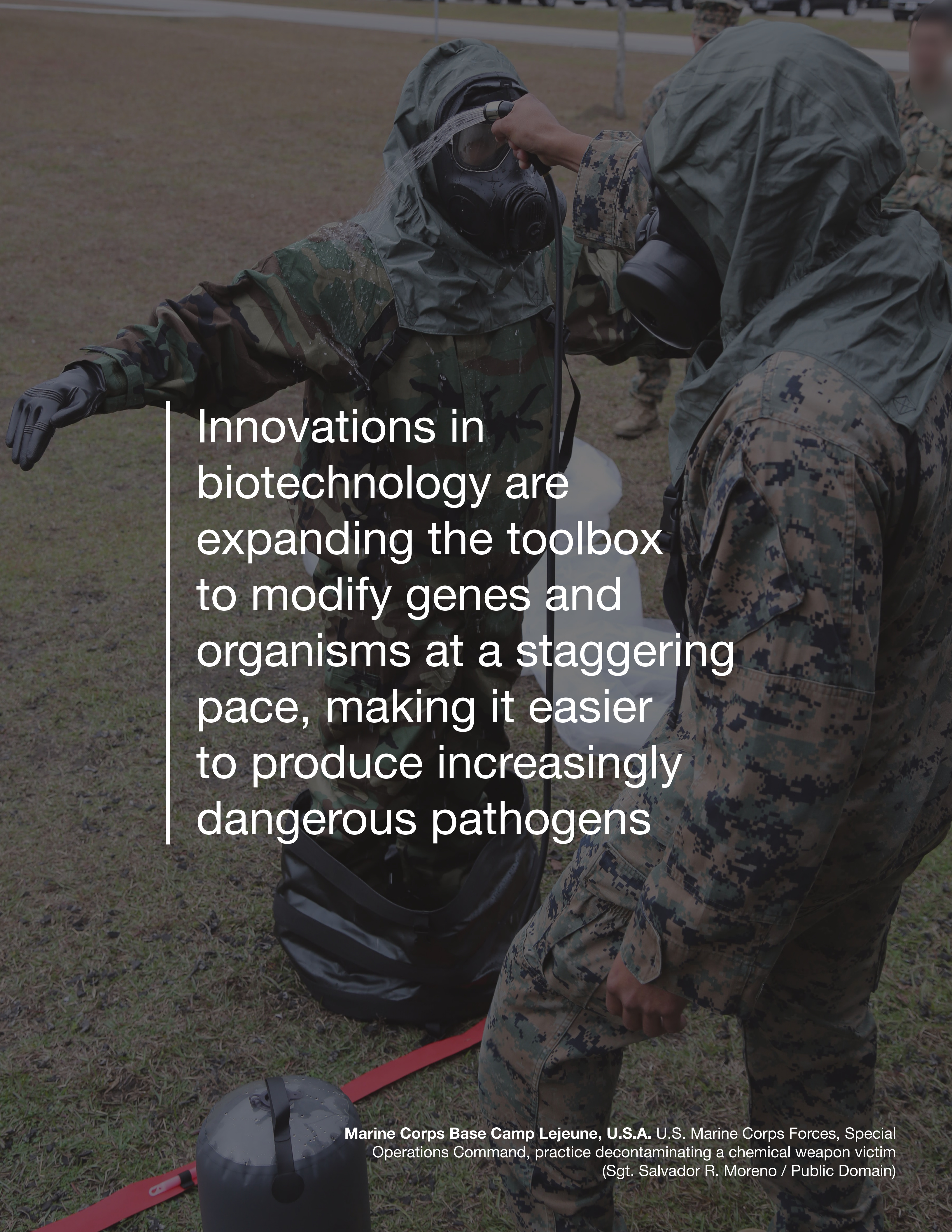
[1] "India Successfully Test Fires Nuclear-Capable Agni-5 Missile." NDTV.com. <https://www.ndtv.com/india-news /india-successfully-test-fires-nuclear-capable-agni-5-missile-1960649> (Accessed February 1, 2019).

[2] Kristensen, Hans M., and Robert S. Norris. "Chinese Nuclear Forces, 2018." Bulletin of the Atomic Scientists 74, no. 4 (July 4, 2018): 289–95. <https://doi.org/10.1080/00963402.2018.1486620>.

[3] Kristensen, Hans M., and Matt Korda. "Indian Nuclear Forces, 2018." *Bulletin of the Atomic Scientists* 74, no. 6 (November 2, 2018): 361–66. <https://doi.org/10.1080/00963402.2018.1533162>.

## Lt. Gen. (Dr.) Prakash Menon, PVSM, AVSM, VSM

Lt. Gen. (Dr.) Prakash Menon, PVSM, AVSM,VSM served for 40 years in the Indian Army. Extensive operational experience in Jammu & Kashmir including the Siachen Glacier. Awarded three Distinguished Service awards. Former Military Adviser in India's National Security Council Secretariat. Presently Director, Strategic Studies Programme, Takshashila Institution, Bangalore and Adjunct Professor, National Institute of Advanced Studies, Bangalore. Elected member of the Executive and Governing Council of Institute of Defense Studies & Analysis (IDSA) and United Service Institution (USI), New Delhi.



Innovations in biotechnology are expanding the toolbox to modify genes and organisms at a staggering pace, making it easier to produce increasingly dangerous pathogens

**Marine Corps Base Camp Lejeune, U.S.A.** U.S. Marine Corps Forces, Special Operations Command, practice decontaminating a chemical weapon victim (Sgt. Salvador R. Moreno / Public Domain)

# Re-thinking Biological Arms Control for the 21st Century

Dr. Filippa Lentzos

International treaties prohibit the development and use of biological weapons. Yet concerns about these weapons have endured and are now escalating. It is high time to take a hard look at technical and political developments and consider how the international security policy community should respond.

A major source of the growing concern about future bioweapons threats stem from scientific and technical advances. Innovations in biotechnology are expanding the toolbox to modify genes and organisms at a staggering pace, making it easier to produce increasingly dangerous pathogens. Disease-causing organisms can now be modified to increase their virulence, expand their host range, increase their transmissibility, or enhance their resistance to therapeutic interventions.[1] Scientific advances are also making it theoretically possible to create entirely novel biological weapons,[2] by synthetically creating known or extinct pathogens or entirely new pathogens.[3] Scientists could potentially enlarge the target of bioweapons from the immune system to the nervous system,[4] genome, or microbiome,[5] or they could weaponize 'gene drives' that would rapidly and cheaply spread harmful genes through animal and plant populations.[6]

Concurrent developments in other emerging technologies are also impacting potential future biological weapons threats. Developments in artificial intelligence and machine learning could speed up identification of harmful genes or DNA sequences. Artificial intelligence and machine learning could also potentially enable much more targeted biological weapons that would harm specific individuals or groups of individuals based on their genes, prior exposure to vaccines, or known vulnerabilities in their immune system.[7] Big Data and 'cloud labs' (completely robotized laboratories for hire) facilitate this process by enabling massively scaled-up experimentation and testing, significantly shortening 'design-test-build' timeframes and improving the likelihood of obtaining specificity or producing desired biological functionality.[8] Other developments provide new or easier ways to deliver pathogens or biological systems. Nanotechnology could potentially create aerosolized nanobots dispersing lethal synthetic microbes or chem-bio hybrids through the air,[9] or in vivo nanobots releasing damaging payloads inside human bodies.[10] Aerosol or spraying devices attached to swarms of small unmanned aerial vehicles, or drones, could be another potential means to disperse biological agents. Additive manufacturing, or 3D printing, could circumvent barriers imposed by national export control systems on controlled laboratory equipment or dispersal devices.

Developments in the biological sciences and other emerging technologies mean that it is easier to misuse the science for a larger group of people, that attack surfaces and vulnerabilities are becoming greater, that there is an expanding 'gray area' between permitted defensive activities and banned offensive activities, and that it is becoming harder to detect and attribute bioweapons use.

The political backdrop to these technical advances in biotechnologies and other emerging technologies is also important. There is increased worldwide militarization, with global military spending at an all-time high since the fall of the Berlin Wall.[11] Unrestrained military procurement and modernization is creating distrust and exacerbating tensions. In the biological field, the proliferation of increasingly sophisticated biodefense capacities, within and among states, can lead to nations doubting one another's intentions.[12] Such doubts could potentially result in bioweapons capabilities and, ultimately, bioweapons use. Another facet of the political backdrop is the increasingly multipolar world in which rising powers view the use of force, the post-war rules-based international system, human rights, and justice differently, and they appear to be actively seeking to undermine the established order. Significant non-state actors, from the private sector to foundations to 'super-empowered' individuals, are also wielding a growing influence over world politics and decision-making processes and have unprecedented technological opportunities to carry out attacks and disrupt societies.[13]

The repeated use of chemical weapons on the battlefield and against civilian populations, particularly in Syria, is significantly undermining the chemical weapons convention, and there are many who are concerned this might also undermine the norm against biological weapons enshrined in the Biological Weapons Convention. In theaters of war, there has been no known use of biological weapons since WWII, when there were substantial covert attacks on China by Japan, as well as some clandestine use in Europe against Germany. While no states are accused of maintaining biological weapons programs, and the multilateral treaty prohibiting biological weapons now has 182 states parties and it is still gaining membership, the U.S. intelligence community has asserted that advances in biology, and particularly in genome editing technologies, pose a threat to U.S. national security. In its 2016 assessment of threats to U.S. national security, James R. Clapper, the then-Director of National Intelligence, stated: "Given the broad distribution, low cost, and accelerated pace of development of [genome editing], its deliberate or unintentional misuse might lead to far-reaching economic and national security implications."[14] A recent National Academy of Sciences committee, funded by the U.S. Department of Defense to develop a framework to systematically assess threats from genome editing, claimed "it is possible to imagine an almost limitless number of potential malevolent uses" for the technology and other synthetic biology technologies.[15]

The U.S. intelligence community is clearly worried an adversary might be harnessing techniques for sequencing, synthesizing, and manipulating genetic material for offensive use, and the government is investing heavily in defensive capabilities. The Defense Advanced Research Projects Agency (DARPA), the U.S. military's research wing, asserts that "the application of biotechnologies by an adversary is an area where the United States could be most surprised as a nation, but it is also a source of great potential, where the United States could develop a host of new surprises of its own."[16] The goal to "harness biology as technology" is one of four main areas of focus for DARPA's strategic investments in 'overmatch' capabilities.[17] In a Congressional testimony from March 2017, Arthur T. Hopkins, Acting Assistant Secretary of Defense for nuclear, chemical, and biological defense

**Deir ez-Zor, Syria.** A destroyed ISIL chemical weapons factory (Zana Omar / Public Domain) programs, stated that: “The same tools of synthetic biology that we’re concerned about as being capable of being used against us, we are also using in the laboratories to help develop countermeasures.”[18] This build-up of biodefense infrastructure and capacities, not just in the United States but taking place around the world, means that states are moving closer to being in a position to threaten or perpetrate a biological attack.

Considering all of this, how can the international security policy community continue to devalue biological weapons as a military option? The Biological Weapons Convention and its norms need to be reinforced and evolved. New working practices must be developed and stakeholder involvement must be increased. A science advisory board must be established. New mechanisms for building trust and managing perceptions of intent in biodefense must be implemented. Guidelines on biological research with high misuse potential must be developed.

Yet, to be fit for the 21st century, biological arms control will also require new thinking about the structures and actors involved. One possibility could be to develop a network of influence, composed of exceptional individuals from business, academia/science, politics, defense, civil society, and international organizations, to act as a ‘global board of trustees’ to oversee developments in science, business, defense, and politics relevant to the biological threats and decide on concerted cross-sector actions. This board of trustees could be complemented by enrolling exceptional individuals and select institutions to act as ‘sentinels.’ These sentinels would have dual functions: to actively promote responsible science and innovation, and to identify security risk for consideration by the global board of trustees. These new governance structures could be supplemented by various initiatives, such as an initiative on artificial intelligence and Big Data to establish a new type of transparency, confidence-building, and BWC compliance assessment, and to support the prevention and management of any biological weapons use. None of this, however, would be possible without a group of states to champion responsible bio-innovation. It is time for governments to step up.

[1] Inter-Academy Partnership (2015) The Biological and Toxin Weapons Convention: Implications of advances in science and technology Royal Society and National Academy of Sciences (2016) Trends in synthetic biology and gain of function and regulatory implications.
[2] Caves, John P. Jr. and Seth W. Carus (2014) The Future of Weapons of Mass Destruction: Their Nature and Role in 2030 National Defense University Center for the Study of Weapons of Mass Destruction Occasional Paper No. 10.
Lentzos, Filippa (2017) ‘Ignore Bill Gates: Where bioweapons focus really belongs’ *The Bulletin of Atomic Scientists*, online 3 July 2017.
[3] National Academies of Sciences (2018) Biodefense in the Age of Synthetic Biology
[4] Bruner, Robert and Filippa Lentzos (2017) ‘Neuroscience–and the new weapons of the mind’ *The Bulletin of Atomic Scientists*, online 27 October 2017.
[5] Kirkpatrick, Jesse et al (2018) Editing Biosecurity: Needs and Strategies for Governing Genome Editing.
[6] Ben Ouagrham-Gormley, Sonia and Kathleen M. Vogel (2016) ‘Gene drives: The good, the bad, and the hype’ *The Bulletin of Atomic Scientists*, online 14 October 2016.
[7] National Academies of Sciences (2018) Biodefense in the Age of Synthetic Biology.
[8] Dunlap, Garrett and Pauwels, Eleonore (2017) The intelligent and connected bio-labs of the future: promise and peril in the fourth industrial revolution, Wilson Center Briefs.
[9] Snow, Jennifer and James Giordano (2019) ‘Aerosolized Nanobots: Parsing Fact from Fiction for Health Security—A Dialectical View’, *Health* Security Vo.17(1).
[10] Lentzos, Filippa and Cédric Invernizzi (2018) ‘DNA origami: Unfolding risk?’ *The Bulletin of Atomic Scientists*, online 25 January 2018.
[11] https://www.sipri.org/sites/default/files/2018-06/yb_18_summary_en_0.pdf
[12] https://thebulletin.org/2018/07/darpas-prepare-program-preparing-for-what/.
[13] http://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf.
[14] Senate Armed Services Committee, *Worldwide Threat Assessment of the US Intelligence Community, Statement for the Record*, James R. Clapper, Director of National Intelligence, 9 Feb. 2016, <https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf>.
[15] Committee on Strategies for Identifying and Addressing Biodefense Vulnerabilities Posed by Synthetic Biology, *A Proposed Framework for Identifying Potential Biodefensevulnerabilities Posed by Synthetic Biology: Interim Report* (National Academies Press: Washington, DC, 2017), <https://www.nap.edu/catalog/24832/a-proposed-framework-for-identifying-potential-biodefense-vulnerabilities-posed-by-synthetic-biology>.
[16] DARPA, *DARPA, 1958–2018* (Faircount Media Group: Tampa, Fl., 2018), <https://issuu.com/faircountmedia/docs/darpa_publication/1?ff>.
[17] https://thebulletin.org/2018/04/how-do-we-control-dangerous-biological-research/.
[18] Pellerin, C., “DoD Officials Discuss Countering WMD, Threats Posed by Synthetic Biology,” *US Department of Defense News*, 23 Mar. 2017, <https://www.defense.gov/News/Article/Article/1128356/dod-officials-discuss-countering-wmd-threats-posed-by-synthetic-biology/>.

## Dr. Filippa Lentzos

Filippa Lentzos, Ph.D., is a Senior Research Fellow at King’s College London specializing in biosecurity and biological arms control. She is also an Associate Senior Researcher within the Armament and Disarmament Programme at the Stockholm International Peace Research Institute (SIPRI), a biosecurity columnist at the *Bulletin of the Atomic Scientists*, an Associate Editor of the journal *BioSocieties*, and the NGO Coordinator for the Biological and Toxin Weapons Convention. For more about her work see www.filippalentzos.com.

The process of technological progress and diffusion has played an important—if sometimes inadvertent—role in exacerbating security tensions in the global commons

**Puckapunyal, Australia.** A Chinese People's Liberation Army senior officer (left) shakes hands with senior Japan Ground Self-Defense Force officials (right) (Tech. Sgt. Michael R. Holzworth / Public Domain)

# Technology and Tensions in the Global Commons

Dr. Kristi Govella

For most of history, the domains of the global commons were unclaimed, largely because the technology to access and utilize them did not exist.[1] In areas such as the high seas and outer space, it was impossible for states to establish and maintain sovereign control. Even as the relevant technologies developed, costliness and controls kept them initially concentrated largely in the hands of just a few major powers such as the United States and the Soviet Union. For the United States, "command of the commons" became the military foundation of its hegemony, granting it the ability to access much of the planet and to credibly threaten to deny the use of such spaces to others.[2] Bipolar competition between the United States and the Soviet Union strongly influenced developments in the maritime and outer space domains. In the case of cyberspace, a more recent addition to the traditional global commons, the United States was also initially dominant due to its role in pioneering associated technologies. However, over time and particularly since the end of the Cold War, continuing technological innovation and diffusion have made these domains accessible to a growing number of countries.

This technological progress was born of both cooperation and competition between states. While some states chose to develop certain technologies indigenously, many acquired knowledge and equipment from abroad. Globalization of industry has made it easier for states to obtain a variety of foreign technologies, even lowering the threshold for them to procure disruptive military capabilities. In addition, over the last two decades, American primacy has been increasingly challenged by the rise of China, which has impacted the dynamics of technological development and diffusion across multiple domains. As China has acquired the technology to become more active in the commons, it has prompted major regional powers, such as Japan and India, to accelerate their own technological advancement, and other mid-sized and smaller countries have also become increasingly engaged.[3]

The consequence of this multiplication of technologically sophisticated actors has been the erosion of American primacy in the global commons. Although the United States still remains the most dominant player, it is faced with a more densely populated field, and management of these spaces has become more difficult. This article examines this trend in the high seas, outer space, and cyberspace since the end of the Cold War, with attention to the ways in which the rise of China and the relative decline of the United States have catalyzed greater engagement with the commons, particularly among the countries in Asia that find themselves most affected by this power transition. I argue that advances in and diffusion of technology have transformed the global commons into increasingly crowded domains characterized by interstate competition and heightened tensions. Whether these tensions prevail depends on the creation and strengthening of regimes to manage interactions and promote shared rules and norms.

## THE HIGH SEAS

On the high seas, American preeminence has been challenged by an increasing number of countries that are pursuing the technology to equip maritime forces capable of sustained operation across the deep waters of the ocean.[4] Much attention has focused on the technological advances made by China as a rising power seeking to modernize its naval forces. Since the 1990s, China's navy has rapidly expanded to more than 300 ships, and it has also heavily invested in submarines, with roughly 80 in total today.[5] It put to sea its second aircraft carrier, the first domestically-built, in April 2018. In addition, reports indicate that the Chinese navy is currently working toward "technological breakthroughs in nuclear-powered aircraft carriers, new nuclear-powered submarines, quieter conventionally powered submarines, underwater artificial intelligence-based combat systems and integrated networked communications systems… in line with the service's aim of becoming a networked, blue water navy by 2025."[6] Although China still lacks the ability to project naval power on a global scale, it has strategically focused its efforts on developing the ability to challenge the United States in key places such as the Taiwan Strait and the South China Sea. Its efforts include pursuing anti-access capabilities such as radar, satellites, and missiles intended to neutralize some of the advantage possessed by powerful American aircraft carrier strike groups.[7] For example, high-speed ballistic missiles like the DF-26, known as “carrier killers,” are designed to strike moving ships as far away as Guam, and the YJ-12B anti-ship cruise missile that China has deployed in the South China Sea can reach the waters between Vietnam and the Philippines.[8]

Other countries in the region have made similar upgrades to their naval technology, prompted by increased Chinese activity as well as by their own domestic concerns, and as a result, it is increasingly the case that major regional players in Asia have the ability to dominate their immediate neighborhoods.[9] Large-deck vessels and submarines have proliferated across the region. For example, the Indian navy is undergoing modernization, with plans to become a 212-warship force by 2027 to guard India’s geo-strategic interests, though funding has been a challenge. Despite the fact that Japanese spending on its Maritime Self-Defense Force is limited by its constitution and associated policy constraints, Japan has expanded its submarine fleet and indigenously developed maritime patrol aircraft to replace its aging stock. Plans are underway to convert Japan’s two largest warships, the Izumo and the Kaga, into aircraft carriers.[10] South Korea has also been modernizing its navy and in October 2018 announced plans to create a blue-water fleet consisting of three squadrons and advanced Aegis destroyers. South Korea also launched the first of a planned fleet of nine indigenously designed KSS-III diesel-electric attack submarines in September 2018.

In Southeast Asia, Vietnam, the Philippines, and Malaysia have modernized and upgraded their maritime capabilities in response to increased Chinese presence in the disputed waters of the South China Sea. As China has engaged in land reclamation activities to build up small features in the area and erected infrastructure such as naval docks, landing strips, and radar and communications systems atop them, other claimant nations have come to feel that they too need increased naval capabilities to cope with Chinese assertiveness. Some of these efforts have been supported by Japan, which has donated used vessels and provided training to Southeast Asian countries as part of its defense capacity building program.[11] Other Southeast Asian countries are also active in the maritime domain. Singapore has steadily invested in defense procurement due to its persistent sense of vulnerability, with recent acquisitions including new submarines featuring more firepower and combat options.[12] Indonesia has also begun modernizing its naval forces in an effort to keep up with Singapore and Malaysia.[13] As a consequence of technological development and diffusion, the amount of interaction and tension on the high seas has intensified. The maritime order is increasingly a multipolar one, with many

**Yokohama, Japan.** The JS Izumo leaves Yokohama Port (椎林 隆夫 / CC BY-SA 4.0) players powerful enough to pursue their own interests, at least in their own neighborhoods. While this may be most evident in the South China Sea, it is also playing out in oceans as far-flung as the Arctic, where increased Chinese and Russian activity have also elicited more engagement from Japan and other countries.

## OUTER SPACE

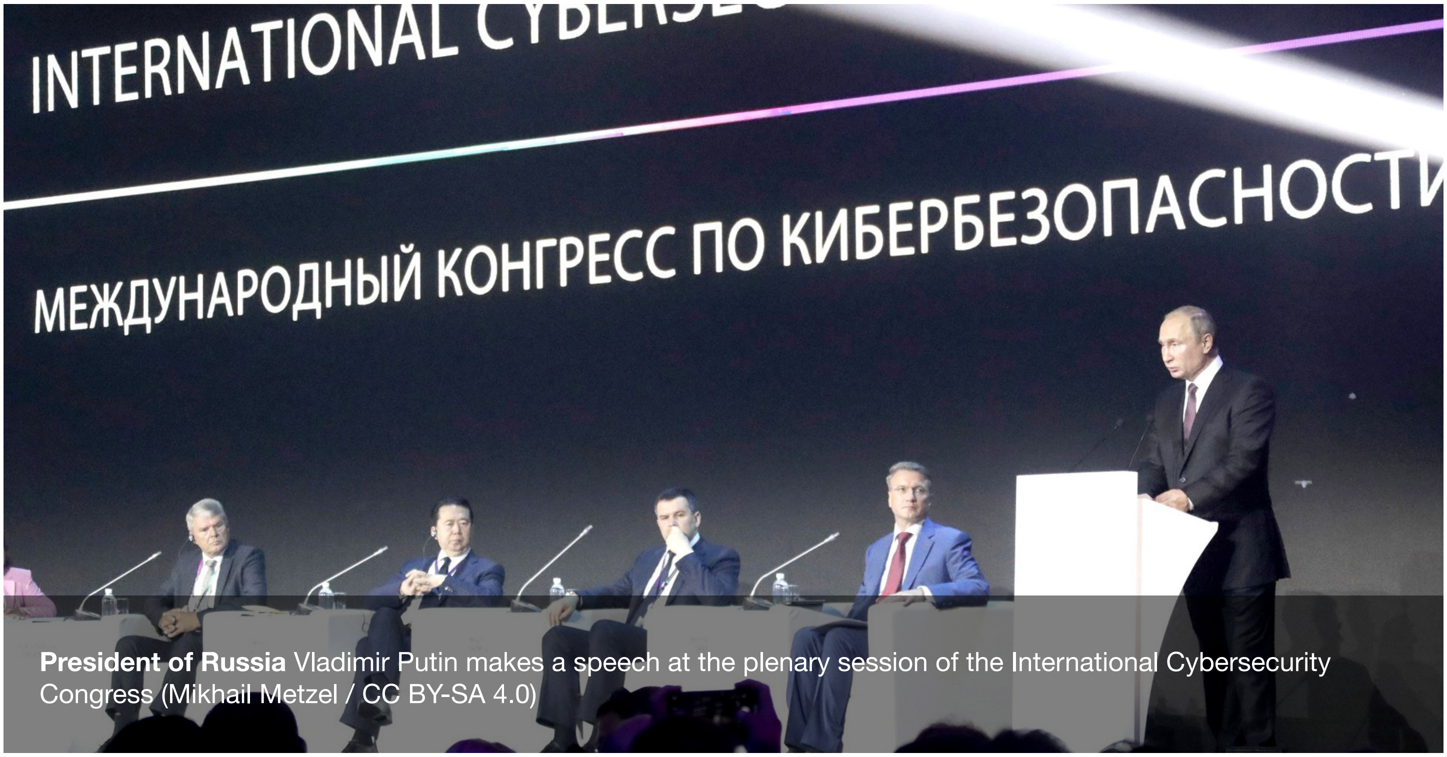
Far above the oceans, a similar pattern of technological progress and diffusion has emerged on another plane of the global commons: outer space. Although the United Nations took the position that outer space was to be used only for peaceful purposes and not subject to territorial claims by individual states, the domain was strongly shaped by the space race between the United States and the Soviet Union that began with the launch of Sputnik I in October 1957.[14] For decades, the United States and the USSR were the dominant players in outer space until the end of the Cold War ceded the advantage to the United States. Over time, American predominance in this domain has gradually begun to erode due to internal budget pressures and growing competition from other states. Outer space offers states many opportunities to gain international prestige, to engage in cutting-edge research, and to launch satellites to facilitate military and civilian communications. Despite the high costs of developing space capabilities, late-developing countries have benefited from the ability to leapfrog developmentally by purchasing foreign space technology, avoiding the expensive mistakes inherent in trying to develop these complex technologies indigenously.[15]

As a result of this technological diffusion, a greater number of countries have become active in outer space, and as in the maritime domain, many of the academic and policy conversations have focused on the rise of China. China formally launched its manned space program in 1992, and it became the third country in history to launch a human into space in 2003. In 2007, it successfully conducted a direct anti-satellite (ASAT) weapon exercise, prompting concern that it might direct this new ability toward the satellites of other nations. China has explicitly linked its space program to its national security, and its activities have continued to expand. It plans to build a space station to support its long-term goals for space exploration and announced the first opportunity for all United Nations countries to apply to be involved in science missions in 2018, with the first module planned to launch in 2020. In January 2019, China became the first country to land a probe on the far side of the moon, a move that some link to plans for future exploitation of space resources.[16]

Chinese actions have prompted renewed competition, as other countries have sought both the technological capacity and the policy tools to become more active in outer space. While Japan had long possessed relatively sophisticated space capabilities, the Chinese ASAT test and North Korean ballistic missile tests provoked it in 2008 to revise the domestic laws that had restricted its space program to peaceful purposes. This enabled Japan to procure a host of advanced military space capabilities to match or even exceed those of China, including dual-use assets in launch systems, communications and intelligence satellites, and counterspace capabilities.[17] Similarly, India has pursued a civil space program for decades, but technological advances by China and others have led it to expand its activities, to fund high-prestige exploratory missions, and to begin conducting military space activities. South Korea has rapidly developed its space capabilities since the early 1990s, focusing initially on satellite development, and more recently, on space launch vehicles. Other countries such as Australia, Indonesia, Malaysia, North Korea, Pakistan, the Philippines, Singapore, Taiwan, Thailand, and Vietnam are also beginning to play a significant regional or international role in space.[18] In addition, the United States has framed some of its recent activities in outer space as a response to challenges from China and Russia, with President Trump's 2018 proposal for the creation of a new Space Force as a sixth branch of the armed forces prompting Chinese criticism that the United States itself is promoting the weaponization of space.[19]

## CYBERSPACE

The role of technology is perhaps even more obvious in cyberspace, a relatively new addition to discussions of the global commons. Unlike outer space or the high seas, cyberspace is a virtual domain entirely constituted by technology; however, it is also more tangible than the other domains in some ways, since specific parts of its physical networks and infrastructure are actually owned by states and private actors. Advocates of including cyberspace as a new domain of the global commons point to the ways in which cyberspace is vast and difficult to control, as well as to the utility gained from its free and open use. Others claim that cyberspace is more akin to



**President of Russia** Vladimir Putin makes a speech at the plenary session of the International Cybersecurity Congress (Mikhail Metzel / CC BY-SA 4.0)

territorial seas to which access can be denied and argue that unfettered global access is no longer possible nor desirable.[20] While this definitional debate remains unresolved, there is growing consensus that the maritime, air, outer space, and cyberspace domains are fundamentally strategically interconnected.[21] Developments in cyberspace are not divorced from consequences in the physical world; cyber capabilities are often seen as complementary to military advances, for example, and attacks in the cyber realm can be used to destroy and disable physical infrastructure.

Research funded by the American government led to the creation of the Internet in the 1980s, and the United States was clearly the dominant player in the early days of cyberspace. However, in this domain as well, advances in and diffusion of technology have transformed cyberspace into a fundamentally more competitive virtual arena. In addition to boasting one of the world's fastest growing Internet economies, China is also home to one of its most active cyber operations programs. In the military realm, China has made a concerted effort to develop cyberspace capabilities to close the gap with the United States as part of its anti-access area denial strategy, for example. American policymakers have voiced concerns about these developments and attempted to fortify themselves against potential attacks, though analysts point out that China itself also has a number of vulnerabilities.[22] Many also criticize China for its undemocratic policies in cyberspace, including censorship and surveillance of its citizens, as well as for increasing reports of Chinese economic espionage and intelligence gathering over the Internet. As highlighted by the events surrounding the 2016 American presidential election, Russia has also developed a highly advanced offensive cyber program that American intelligence chiefs have said "poses a major threat to U.S. government, military, diplomatic, commercial, and critical infrastructure and key resource networks."[23]

In cyberspace, technology can be a force multiplier that replicates the existing hierarchy of power, but it can also have a leveling effect, mitigating some of the advantages traditionally possessed by major powers and allowing smaller states and even non-state actors with limited resources to go on the offensive.[24] For example, fairly modest technological advances have enabled North Korea to become a major threat in the cyber realm. North Korea's cyber operations are deliberate top-down efforts to target states that rely heavily on cyberspace for national and military activity, like the United States and South Korea.[25] North Korea is able to engage in these targeted attacks at a relatively low cost and low risk to itself in comparison to what it might face in engaging in other forms of conflict. Non-state actors have also emerged as threats in cyberspace, sometimes independently and sometimes working in tandem with governments, as in the case of China's cyber militias and "patriotic hackers."[26]

In recognition of these growing threats from both state and non-state actors, many other countries have moved to acquire the technology to develop their own cybersecurity programs. Largely in response to China, Japan has moved to develop its own domestic policy infrastructure and capabilities for defensive cybersecurity and to incorporate cyberspace into the scope of the United States-Japan alliance.[27] Focused primarily on North Korea, South Korea has also developed its cybersecurity policy infrastructure and strengthened its security protocols following several high-profile hacking incidents, including attacks on government agencies and on Korea Hydro and Nuclear Power in 2014. The countries of Southeast Asia have been slower to respond to the threats and opportunities of cyberspace due to the wide variation in their technological and institutional capabilities, but there has been some recent progress. As the sub-region's most technologically advanced country, Singapore has driven much of the cybersecurity agenda of the Association of Southeast Asian Nations.[28] Other Southeast Asian countries have engaged in specific national cybersecurity activities, such as Malaysia, which has held annual public-private exercises to enhance its ability to protect critical infrastructure from cyber attacks. As in the case of the high seas and outer space, as more states and private actors have gained the technological capability to become active in cyberspace, it has become more difficult to ensure the safety and stability of this domain.

## IMPLICATIONS FOR POLICY

This examination of these three domains of the global commons—the high seas, outer space, and cyberspace—illustrates how first technological innovation and then subsequent technological diffusion have made accessible places and spaces that were previously largely inaccessible. In the early days of these domains, though no single country claimed sovereignty over them, they were dominated by the United States and, in the case of the high seas and outer space, by the Soviet Union as well. However, with the end of the Cold War and the rise of China, these domains appear to be becoming increasingly multipolar. In some ways, this pluralization of the global commons through technology is positive in that more countries than ever have the ability to utilize them and their resources. However, as the countries that are active in these domains become more numerous, their interactions are also creating competitive dynamics that impact the security environment, particularly because the technological capacity of states to engage in the commons has developed more quickly than the regimes for their effective governance.

Although technology alone did not create these frictions between countries, many of which are rooted in long histories of complex interactions, the process of technological progress and diffusion has played an

**Tokyo, Japan.** 18th Chairman of the Joint Chiefs of Staff Gen. Martin E. Dempsey and Prime Minister of Japan Shinzō Abe talk during a bi-lateral meeting (U.S. Navy Petty Officer 1st Class Daniel Hinton / Public Domain) important—if sometimes inadvertent—role in exacerbating security tensions in the global commons.[29] To some extent, just the fact that a newcomer is acquiring the technology to become active in a domain may make other states feel threatened. The global commons are resource domains to which all nations have legal access, but they contain different kinds of resources that are subject to varying levels of excludability and subtractability.[30] Though it is often difficult to exclude others from using resources, each additional appropriator may reduce the amount of resources left for others, leading states to feel compelled to compete.

In addition, the specific nature of technological developments in the global commons has a tendency to exacerbate security dilemma dynamics in these domains. A key part of the security dilemma is that states are not explicitly trying to change the status quo; rather, their defensive intentions in developing or acquiring new technologies are difficult to credibly signal in an anarchic environment of uncertainty and mistrust, which results in misinterpretation by others.[31] Many of the technologies that have enabled states to become more engaged in the global commons are difficult to distinguish in terms of a state's offensive and defensive capabilities, further triggering this security dilemma logic. For example, due to the dual-use nature of space technologies, there is often inherent ambiguity to advances; civil and military uses cannot be truly separated. Therefore, the increasing technological sophistication of one state is perceived to decrease the security of other states, which in turn feel that they need to respond with similar technological countermeasures to defend themselves.[32] Moreover, while situations where defensive technologies have the advantage can be stabilizing, many countries feel that offensive forces may have the advantage in these domains, which further drives the acquisition of technologies that worsen the security dilemma.[33] Although the states discussed here are not engaged in the kind of full-scale arms race that can result from this action-reaction sequence, a clear trend toward competitive behavior has emerged. In terms of military competition in the areas of the commons addressed in this article, these dynamics are most pronounced in the maritime domain at present.

A pressing challenge for the future is that all of these domains are in need of stronger regimes that could help ameliorate the security dilemma and ensure the good governance of the commons for the benefit the international community as a whole. The lack of a governing authority over the global commons and the misleading notion of their limitlessness make them particularly vulnerable to the current shifts in the international system.[34] Although the rules and norms of the high seas are the most developed of the domains discussed here, they have been increasingly challenged by the activities of states such as China, as seen with recent discussions surrounding the UN Convention on the Law of the Sea in the context of the South China Sea territorial disputes. The outer space regime grounded in the 1967 Outer Space Treaty needs a great deal more development to protect countries not only from anti-satellite and kinetic weapons but also from the growing problem of orbital debris, which threatens all space capabilities.[35] Cyberspace is by far the least governed of these three domains, with its own regime still at an embryonic stage. In each of these domains, the development of technologies enabling states to access the commons has outpaced the development of the tools for their governance. Stronger regimes are necessary if only to promote transparency and information sharing, which existing scholarship suggests may help to reassure states, build trust, and reduce the risks of the security dilemma.

As a result of the increasing pluralization of power in the global commons, the United States increasingly depends on the newcomers to these domains to help promote their good governance. As these new players integrate into the existing system, they may come to see benefits from maintaining the stability and accessibility of the global commons, just as the United States did. However, it is likely that promoting shared perspectives regarding the global commons will require concerted effort and persuasion by those states most invested in such regimes. Cooperation between like-minded partners in the maritime, outer space, and cyberspace domains will be essential to protecting their peaceful use and ensuring that they remain open for the benefit of all.

[1] As Vogler points out, "one shared characteristic of the global commons is their close association with scientific discovery and developing technological capability." John Vogler, "Global Commons Revisited," *Global Policy* 3, (1) (2012): 61–71.
[2] Barry Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security* 28, (1) (2003): 5–46.
[3] For example, Japan has responded to increased Chinese activity across all three of the domains of the global commons addressed here. For an extended discussion, see Kristi Govella, "Securing the Global Commons? Japan in Outer Space, Cyberspace, and the High Seas" (Workshop on Conflict, Cooperation, and Interaction in the Global Commons, University of California, Berkeley, 2019).
[4] Kerry Lynn Nankivell refers to these countries as "blue-water middle powers." See for example, Kerry Lynn Nankivell, "A Review of 'Maritime Power and the Law of the Sea: Expeditionary Operations in World Politics': By James Kraska. Oxford:

Oxford University Press, 2011, 484 pp.," *Ocean Development & International Law* 42 (4) (October 2011): 383–87.

[5] China Power Team, "How is China Modernizing Its Navy?" *China Power, December 17, 2018,* < https://chinapower.csis.org/china-naval-modernization/>.

[6] Mike Yeo, "China to Develop Its First Nuclear-Powered Aircraft Carrier," *Defense News*, March 1, 2018, <https://www.defensenews.com/naval/2018/03/01/china-to-develop-its-first-nuclear-powered-aircraft-carrier/>.

[7] See for example, Michael Beckley, "The Emerging Military Balance in East Asia: How China's Neighbors Can Check Chinese Naval Expansion," *International Security* 42, (2) (2017): 78–119.

[8] The United States has in turn responded to Beijing's new anti-access area denial capabilities. See for example, Matteo Dian, "The Pivot to Asia, Air-Sea Battle, and Contested Commons in the Asia-Pacific Region," *The Pacific Review* 28 (2) (2015): 237–57.

[9] For example, Ritter refers to this as a "regional command of the commons." See Tripp Ritter, "The Regional Command of the Commons: Japan's Military Power," *The Korean Journal of Defense Analysis* XVII (1) (2005): 235–58.

[10] Felix Chang, "Japan's New(ish) Aircraft Carriers: Reviving Japanese Naval Aviation," *Foreign Policy Research Institute,* February 1, 2019, <https://www.fpri.org/article/2019/02/japans-newish-aircraft-carriers-reviving-japanese-naval-aviation/>.

[11] See for example, Paul Midford, "Japan's Approach to Maritime Security in the South China Sea," *Asian Survey* 55 (3) (June 1, 2015): 525–47;\\uc0\\u8221{} {\\i{} Asian Survey} 55, no. 3 (June 1, 2015 and Kristi Govella, "Between Aid and Arms: Japan's Emerging Approach to Defense Capacity Building" (American Political Science Association Annual Meeting, Boston, MA, 2018).

[12] Lim Min Zhang, "Singapore Navy Launches First of Its Four New Submarines," *The Straits Times, February 19, 2019, <https://www.straitstimes.com/singapore/spore-navy-launches-first-of-its-four-new-submarines>.*

[13] For a brief overview, see Sheryn Lee, "Crowded Waters: Naval Competition in the Asia–Pacific," APSI Special Report (Australian Strategic Policy Institute, 2015).

[14] It is important to note that the technological advances of this period were also enabled by cooperation. Maiʻa Cross argues that despite very visible competition among the main states involved, outer space was more accurately characterized as the product of international cooperation. See Mai'a Cross, "International Cooperation and Outer Space Exploration" (Workshop on Conflict, Cooperation, and Interaction in the Global Commons, University of California, Berkeley, 2019).

[15] Alexander Gerschenkron, *Economic Backwardness in Historical Perspective* (Cambridge: Belknap Press, 1962).

[16] See for example, Namrata Goswami, "The New Space Race Pits the US against China. The US Is Losing Badly.," *The Washington Post*, January 10, 2019.

[17] Saadia Pekkanen and Paul Kallendar-Umezu, *In Defense of Japan: From the Market to the Military in Space Policy* (Stanford: Stanford University Press, 2010); Paul Kallendar and Christopher Hughes, "Hiding in Plain Sight? Japan's Militarization of Space and Challenges to the Yoshida Doctrine," *Asian Security*, 2018.

[18] For an excellent overview of these developments, see James Clay Moltz, *Asia's Space Race: National Motivations, Regional Rivalries, and International Risks* (New York: Columbia University Press, 2012).

[19] See for example, Tom O'Connor, "China Says Space is Not U.S. 'Private Property' as Donald Trump Plans to Build New Missile Defense There," *Newsweek, February 12, 2019, < https://www.newsweek.com/china-space-property-trump-missile-defense-1329295>.*

[20] Sam Tangredi, "From Global Commons to Territorial Seas: A Naval Analogy for the Nationalization of Cyberspace," *Military Cyber Affairs* 3 (1) (2018).

[21] See for example, Shawn Brimley, "Promoting Security in Common Domains," *The Washington Quarterly* 33, (3) (2010): 119–32.

[22] Jon Lindsay, "The Impact of China on Cybersecurity: Fiction and Friction," *International Security* 39 (3) (2015 2014): 7–47.

[23] Steve Ranger, "US Intelligence: 30 Countries Building Cyber Attack Capabilities," *ZDNet*, January 5, 2017, <https://www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/>.

[24] On cyber technology as a force multiplier, see for example, Simone Dossi, "Confronting China's Cyberwarfare Capabilities: A 'Weapon of the Weak' or a Force Multiplier?," in *US Foreign Policy in a Challenging World*, ed. Marco Clementi, Matteo Dian, and Barbara Pisciotta (New York: Springer, 2018).

[25] Jenny Jun, Scott LaFoy, and Ethan Sohn, *North Korea's Cyber Operations: Strategy and Responses* (Washington, DC: Center for Strategic & International Studies, 2015).

[26] While some of these actors' activities are thought to be state-directed, there has been some research examining the emergence of regime-defending voices among Chinese individuals who are not state agents. For a nuanced account, see Rongbin Han, "Defending the Authoritarian Regime Online: China's 'Voluntary Fifty-Cent Army,'" *The China Quarterly* 224 (December 2015): 1006–25.this project explores the pluralization of online expression in Chinese cyberspace. Following a constituency of internet users who identify themselves as the "voluntary fifty-cent army," the paper explores how these users acquire and consolidate their identity and combat criticism that targets the authoritarian regime. Analysis of the confrontational exchanges between the "voluntary fifty-cent army" and their opponents suggests that a perspective that goes beyond state censorship and regimechallenging activism is required in order to gain a better understanding of online expression in China. Close examination of why and how internet users may voluntarily defend the authoritarian regime also reveals how the dynamics in online discourse competition may work to the authoritarian regime's advantage.","ISSN":"0305-7410, 1468-2648","shortTitle":"Defending the Authoritarian Regime Online","language":"en","author":[{"family":"Han","given":"Rongbin"}],"issued":{"date-parts":[["2015",12]]}}}],"schema":"https://github.com/citation-style-language/schema/raw/master/csl-citation.json"} [27] Paul Kallendar and Christopher Hughes, "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace," *Journal of Strategic Studies* 20, (1–2) (2017): 118–45.

[28] Elina Noor, "ASEAN Takes a Bold Cybersecurity Step," *The Diplomat*, October 4, 2018.

[29] For example, for a discussion of the historical legacies exacerbating the security dilemma in Sino-Japanese relations, see Thomas J. Christensen, "China, the U.S.-Japan Alliance, and the Security Dilemma in East Asia," *International Security* 23 (4) (April 1999): 49–80.

[30] See for example, Susan Buck, *The Global Commons: An Introduction* (Washington, DC: Island Press, 1998).

[31] It is also important to note that in some cases states are actually explicitly trying to change the status quo, which does not follow the logic of the security dilemma. On this point, see Adam P. Liff and G. John Ikenberry, "Racing toward Tragedy?: China's Rise, Military Competition in the Asia Pacific, and the Security Dilemma," *International Security* 39 (2) (October 2014): 52–91.

[32] Robert Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30 (2) (1978): 167–214.

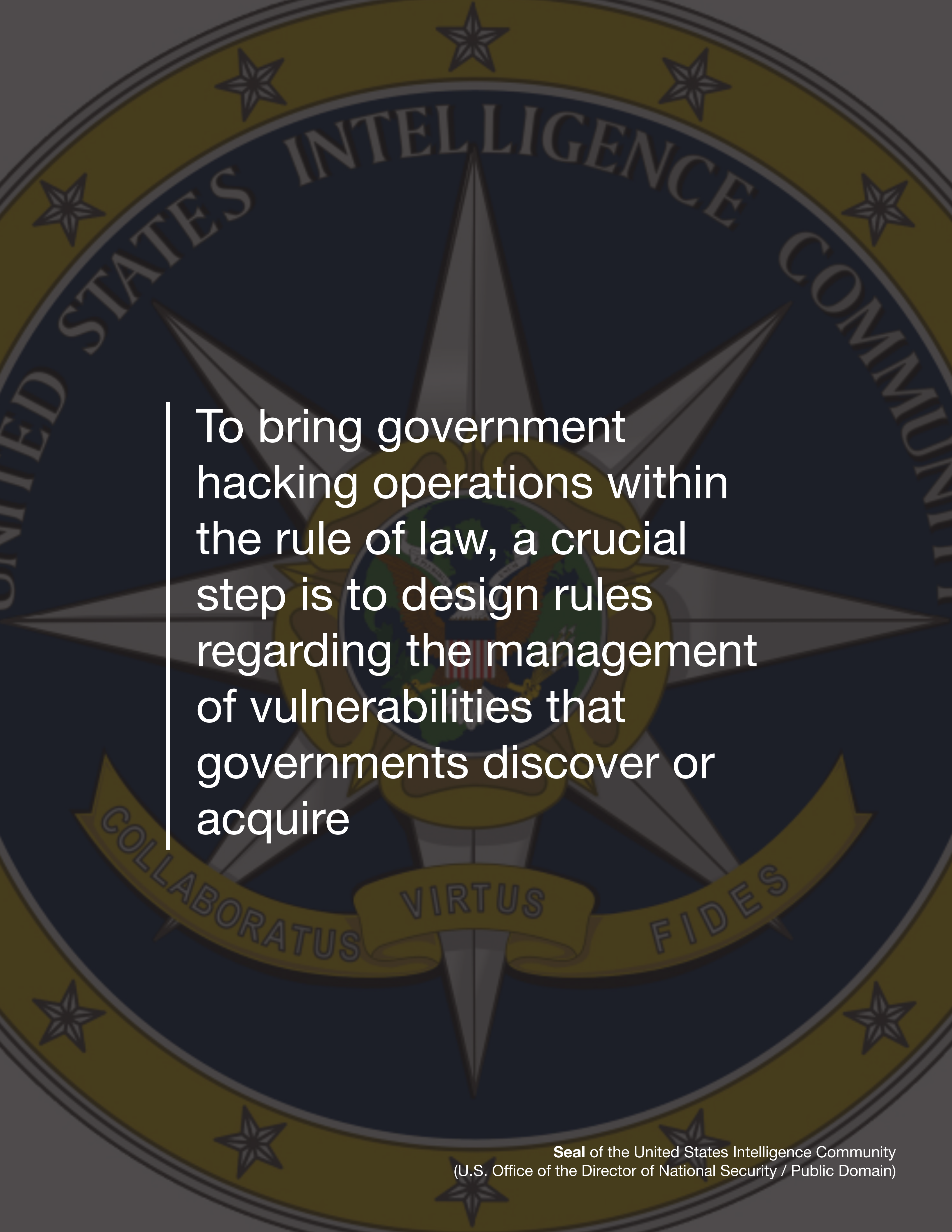
[33] The issue of whether offense or defense has the advantage in cyberspace is still being debated. For a discussion of the advantages of defensive capabilities, see Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," *International Security* 41 (3) (2016): 72–109.

[34] Carla Freeman, "The Fragile Global Commons in a World in Transition," *SAIS Review of International Affairs* 36 (1) (2016): 17–28.

[35] See Abraham Denmark, "Managing the Global Commons," *The Washington Quarterly* 33 (3) (2010): 165–82.

# Dr. Kristi Govella

Dr. Kristi Govella is an Assistant Professor in the Asian Studies Program at the University of Hawaiʻi at Mānoa, a National Asia Research Program Fellow, and an Adjunct Research Fellow at the East-West Center. Her work deals with the intersection of economics, politics, and security in Asia, with a particular focus on Asian regionalism and Japanese politics. She is currently working on a number of projects related to economics-security linkages, regional institutional architecture, trade agreements, multinational firms, recent Japanese security reforms, and the global commons. Her publications include ***Linking Trade and Security: Evolving Institutions and Strategies in Asia, Europe, and the United States*** (2013). Prior to joining the University of Hawaiʻi, Dr. Govella was a Postdoctoral Fellow at Harvard University and an Associate Professor at the Daniel K. Inouye Asia-Pacific Center for Security Studies. She holds a Ph.D. and an M.A. in Political Science from the University of California, Berkeley and a B.A. in Political Science and Japanese from the University of Washington.



> To bring government hacking operations within the rule of law, a crucial step is to design rules regarding the management of vulnerabilities that governments discover or acquire

**Seal** of the United States Intelligence Community
(U.S. Office of the Director of National Security / Public Domain)

# The Need for Countries to Establish Robust and Transparent Vulnerabilities Equities Processes

Sharon Bradford Franklin

In 2017, leaders of the U.S. Intelligence Community warned that “more than 30 nations are developing offensive cyberattack capabilities.”[1] This means that more than 30 countries may be conducting hacking operations as a method for surveillance, disruption, or destruction. Unregulated cyber surveillance and cyberattacks by government actors can pose risks not only to a government’s foreign adversaries, but also to its own citizens. Thus, as the United States and other nations work to enhance their own offensive cyber capabilities, as well as to develop strategies to defend against potential attacks, it is critical that these countries establish legal regimes to govern such conduct in cyberspace. Although Germany has established a legal framework to regulate government hacking activities,[2] few countries have done so.[3]

To bring government hacking operations within the rule of law, a crucial step is to design rules regarding the management of vulnerabilities that governments discover or acquire. As with other cyber actors, when governments conduct hacking operations, this frequently involves exploiting vulnerabilities in computer hardware and software systems. But these same flaws can also be manipulated by a government’s foreign adversaries or other malicious actors. Therefore, when countries consider their abilities to rely on hacking as an investigative tool, as well as their interests in exploiting vulnerabilities for military and intelligence operations, they must also evaluate the capacity of information and communications technology providers to repair bugs and protect the cybersecurity of all users. Determining whether to exploit a vulnerability or disclose it to a vendor for patching involves balancing a variety of different security concerns against each other.

Some countries have made progress in formalizing the rules for making these decisions and in publicizing these rules to promote public accountability. In November 2017, the United States released a charter governing its Vulnerabilities Equities Process (VEP), which outlines how the U.S. government weighs the various competing equities.[4] The charter delineates which components of the government will participate in determinations regarding whether to disclose or retain each newly discovered vulnerability, and it sets forth the criteria to be used and the process to be followed in making such assessments. One year later, the United Kingdom (UK) announced its Equities Process, which follows a similar approach.[5] Most recently, in March 2019, Australia released its “Responsible Release Principles for Cyber Security Vulnerabilities,”[6] and Germany is currently working to develop a VEP and is expected to make information about its process public in early 2019.[7] However, as described below, the VEP procedures revealed to date need further improvement,[8] and most of the nations with offensive cyber capabilities have not developed—or at least have not announced—any such framework.

There are several reasons why countries should develop, formalize, and publicize VEP procedures. First, as noted above, creating a VEP is a critical step toward bringing government hacking within the rule of law. Much more work is needed, particularly in the United States, to clarify and limit the authority of government actors to engage in hacking.[9] Nonetheless, clear rules for vulnerability management, transparency regarding the decision-making process, and public reporting of statistics regarding the frequency with which vulnerabilities are disclosed and retained can help hold governments accountable to their citizens. Second, as more countries develop VEP procedures, this can assist nations in cooperating to combat the threats posed by various malicious cyber actors and can help establish international norms. Widespread adoption and publication of VEP rules can facilitate information sharing among countries about common cyber threats, as the United Kingdom has recognized in its Equities Process document, noting that vulnerabilities may not be subject to formal review if they “have already been subjected to similar considerations by a partner and shared with us.”[10] Third, governments will benefit from formalizing decision making to evaluate the security versus security tradeoffs involved in handling vulnerabilities. These are not easy decisions, and, as the "E" in "VEP" recognizes, there are many different "equities" to be assessed in determining when a vulnerability should be disclosed to the vendor for patching. In particular, a VEP can ensure that the interest in disclosing vulnerabilities for repair to promote the cybersecurity of all users will receive appropriate weight and that it will not be lost in the pressured and secretive environment of classified conversations among a limited number of intelligence or military officials.

This last point is worth emphasizing as a critical role to be played by VEP procedures. Despite widespread recognition of the cybersecurity risks posed when governments stockpile vulnerabilities,[11] there can be a natural inclination by law enforcement, intelligence, and military officials to press for retention and exploitation. To ensure a robust VEP that truly weighs all relevant equities, the decision-making process must include adequate representation from government agencies or actors that will press for disclosure and repair of vulnerabilities to promote the public's cybersecurity. For example, the U.S. VEP review board includes the Department of Commerce and the National Cybersecurity Communications and Integration Center, both of which can provide a perspective focused on protecting digital security for all users. Because different nations vary in the structure of their cyber-related operations, VEP procedures should be tailored to individual countries to provide for such representation. The procedures should also ensure that the voices counseling in favor of disclosure and repair will not be regularly drowned out by those urging retention and exploitation.

Although the structure of VEP review boards will likely vary from country to country, there are some critical elements that should be included in any VEP, and the U.S. VEP, the UK Equities Process, and the Australian Responsible Release Principles share certain important features. All three documents explicitly start from the premise that, in most cases, disclosing a vulnerability for repair is in the country's national interest. Promptly disclosing a newly discovered vulnerability to the manufacturer allows companies to develop patches and protect the cybersecurity of all users. As the Australian Responsible Release Principles state: "Our starting position is simple: when we find a weakness, we disclose it."[12] Similarly, all three processes require that any government decision to retain and exploit a vulnerability must be periodically reevaluated on at least an annual basis. Governments must recognize that the vulnerabilities they retain can also be discovered and exploited by their adversaries, and, over time, the cybersecurity risks of leaving vulnerabilities unpatched will continue to grow. As stated in a recent policy paper by the German think tank Stiftung Neue Verantwortung (SNV), VEP policies should determine "'when' and 'how' disclosure should occur rather than 'whether' and 'if.'"[13]

There are also some challenges that are common to any VEP. One difficult issue is the question of whether it should be permissible to exclude a vulnerability from the evaluation process based on a nondisclosure agreement (NDA) with a private vendor. Many countries obtain vulnerabilities by purchasing them from private companies rather than through their own research, and these vendors typically demand NDAs so they can continue to sell the vulnerabilities to other purchasers. Although there is little public information about the scope of this gray market,[14] the U.S. VEP explicitly states that determinations under the process "could be subject to restrictions by partner agreements and sensitive operations."[15] This exclusion of vulnerabilities acquired under NDAs from VEP review threatens to become an exception that swallows the rule. The U.S. government should remove this exemption and require

TDOS Statistics
2014 TDoS Statistics – 260 Incidents Year to Date
TDoS - Criminal Acts by Sector
Comm ISAC Industry Partners

**United States President** Barack Obama tours the National Cybersecurity and Communications Integration Center (Pete Souza / Public Domain) vulnerabilities to be assessed through the VEP, regardless of whether they were discovered by government agencies or purchased from vendors. As some former government officials involved in this process have argued, the government could limit its purchases from vendors to cases where it buys the exclusive rights to a vulnerability, and it could regularly reevaluate these vulnerabilities through the VEP.[16]

Finally, there is the challenge of providing transparency. Certain information about the application of a VEP will appropriately remain classified, such as the nature of vulnerabilities currently being retained for exploitation. But transparency—at least for the applicable rules of the VEP and for statistical information regarding the number of vulnerabilities considered, disclosed and retained—is critical to the legitimacy and successful operation of any VEP. The U.S. VEP charter requires annual reporting, including "statistical data as deemed appropriate,"[17] but the charter does not commit the government to providing its annual report to Congress or the public. Similarly, the Australian Responsible Release Principles state that the Australian Signals Directorate submits annual reports to the Inspector-General and the Minister for Defence, but they do not contain any provision regarding public reporting.[18] The UK Equities Process is completely silent on the issue of transparency reporting. A requirement for regular public reporting should be a high-priority area for improvement to these existing VEP procedures.

The United States, the United Kingdom, and Australia should continue to develop and refine their vulnerabilities review procedures to ensure that all newly discovered vulnerabilities are considered through a robust process that is accountable to the public. Meanwhile, the models provided by these countries are good places for other countries to start. As nations strive to improve their cyber capabilities and grapple with how to best protect their populations and their resources, they should also ensure that their actions are conducted in accordance with the rule of law. Creating clear rules and providing transparency about the management of vulnerabilities can be an important first step in this critical effort.

[1] James R. Clapper, Marcel Lettre, and Michael S. Rogers, *Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States*, 115th Cong., 1st sess., January 5, 2017.
[2] The German Code of Criminal Procedure § 100 (2014).
[3] Alex Betschen, "We're Suing the Government to Learn Its Rules for When It Hacks Into People's Devices," American Civil Liberties Union, December 21, 2018, <https://www.aclu.org/blog/privacy-technology/internet-privacy/were-suing-government-learn-its-rules-when-it-hacks-peoples>.
[4] *Vulnerabilities Equities Policy and Process for the United States Government*, White House document, November 15, 2017.
[5] "The Equities Process," GCHQ, November 29, 2018, <https://www.gchq.gov.uk/features/equities-process>.
[6] "Responsible Release Principles for Cyber Security Vulnerabilities," Australian Signals Directorate, March 2019, <https://asd.gov.au/publications/Responsible-Release-Principles-for-Cyber-Security-Vulnerabilities.pdf>.
[7] Sven Herpig and Ari Schwartz, "The Future of Vulnerabilities Equities Processes Around the World," *Lawfare*, January 4, 2019, <https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world>.
[8] Sharon Bradford Franklin and Andi Wilson, "Rules of the Road: The Need for Vulnerabilities Equities Legislation," *Lawfare,* November 22, 2017, <https://www.lawfareblog.com/rules-road-need-vulnerabilities-equities-legislation>.
[9] Kevin Bankston, "Ending the Endless Crypto Debate: Three Things We Should Be Arguing About Instead of Encryption Backdoors," *Lawfare,* June 14, 2017, <https://www.lawfareblog.com/ending-endless-crypto-debate-three-things-we-should-be-arguing-about-instead-encryption-backdoors>.
[10] "The Equities Process."
[11] Ellen Nakashima and Andrea Peterson, "NSA's use of software flaws to hack foreign targets posed risks to cybersecurity," *The Washington Post,* August 17, 2016, <https://www.washingtonpost.com/world/national-security/nsas-use-of-software-flaws-to-hack-foreign-targets-posed-risks-to-cybersecurity/2016/08/17/657d837a-6487-11e6-96c0-37533479f3f5_story.html>; and "Governments need to do more, and say more, on vulnerability handling," The Cybersecurity Tech Accord, September 10, 2018, <https://cybertechaccord.org/government-vulnerability-handling>.
[12] "Responsible Release Principles for Cyber Security Vulnerabilities."
[13] Sven Herpig, *Governmental Vulnerability Assessment and Management* (Berlin: Stiftung Neue Verantwortung, August 2018), 3.
[14] Rhys Dipshan, "The Federal Policy Loophole Supporting the Hacking-for-Hire Market," *Future Tense*, June 20, 2018, <https://slate.com/technology/2018/06/the-federal-policy-loophole-supporting-the-hacking-for-hire-market.html>.
[15] *Vulnerabilities Equities Policy and Process for the United States Government*, 9.
[16] Ari Schwartz and Rob Knake, *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process* (Cambridge: The Cyber Security Project at the Belfer Center for Science and International Affairs, June 15, 2016), 15.
[17] *Vulnerabilities Equities Policy and Process for the United States Government*, 5.
[18] "Responsible Release Principles for Cyber Security Vulnerabilities," 1.

## Sharon Bradford Franklin

Sharon Bradford Franklin is Director of Surveillance & Cybersecurity Policy at New America's Open Technology Institute (OTI). She leads OTI's work on issues involving government surveillance, encryption, cybersecurity, government access to data, transparency, and freedom of expression online. From 2013 to 2017, she served as Executive Director of the Privacy and Civil Liberties Oversight Board (PCLOB), an independent federal agency that reviews counterterrorism programs to ensure that they include appropriate safeguards for privacy and civil liberties. Previously, she served as Senior Counsel at the Constitution Project, a nonprofit legal watchdog group, working on a range of issues involving national security and privacy and civil liberties. Franklin is a graduate of Harvard College and Yale Law School.

Governments, commercial actors, and private citizens considering new cybersecurity deployment measures either explicitly or implicitly balance the costs to be incurred against the benefits to be derived from the new steps under consideration

**Servers** in a data center
(BalticServers / CC BY-SA 4.0)

# How Much Does a “Privacy” Weigh?

Paul Rosenzweig

Benjamin Franklin is famous, in part, for having said, “Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.” Though historical evidence suggests Franklin’s quote has been misinterpreted,[1] the aphorism has come to stand for the proposition that privacy and security stand in opposition to each other, where every increase in security likely results in a commensurate decrease in privacy, and vice versa.

Couched in those terms, the privacy/security trade-off is a grim prospect. We naturally want both privacy and security to the greatest extent possible. But Franklin tells us this is impossible — that privacy and security are locked in a zero-sum game where the gain of one comes only at the loss of the other.

Of course, this characterization is assuredly flawed; it is certainly possible to adopt systems that maximize both privacy and security in a Pareto optimal way. That is one of the reasons why so many privacy and security experts simply revile the “balancing” metaphor — it obscures more than it illuminates.

But let us, for now, put this debate aside and acknowledge that the balance metaphor is a partially accurate depiction of reality. At least in some instances, increases in security *do* necessitate decreases in privacy, and vice versa. The long-standing debate over encryption technology, for example, appears to be a clear case where tradeoffs are inherent to any policy decision.[2]

This acknowledgment challenges us in many ways, at least one of which has garnered only infrequent notice. It boils down to two questions: How do we measure privacy? How do we measure security? This short commentary highlights these questions and begins to outline some thoughts about its resolution.

These two queries would seem to be natural ones. After all, if we are going to trade security for privacy (or the reverse), we need to assign each a metric value of some sort in order to judge whether the tradeoff is worthwhile. Most people, for example, might be willing to trade a tiny bit of privacy for a thousand-fold increase in security. Conversely, most would not likely be willing to sacrifice substantial privacy for a negligible security gain.

Buried in that commonsense consensus are some hard issues of measurement: What is a “tiny bit”? How do we measure a “thousand-fold increase”? And what makes something “substantial” or “negligible?”

## MEASURING SECURITY

How do we quantify security? This fundamental question underlies almost all modern national and commercial security decisions. The cost-benefit analysis inherent in measuring security drives decisions on new car safety devices, airplane maintenance schedules, and the deployment of border security systems. Indeed, in a world where resources are finite, some assessment of risk necessarily attends any decision — whether implicitly or explicitly.

What is true generally is equally true in the field of cybersecurity. Governments, commercial actors, and private citizens considering new cybersecurity deployment measures either explicitly or implicitly balance the costs to be incurred — whether monetary or in terms of changes to enterprise efficiency — against the benefits to be derived from the new steps under consideration.

The problem with this rather straightforward account of enterprise decision-making is that no universally recognized and generally accepted metric exists to measure and describe security improvements. Unlike, say, the science of electricity, where the general safety of a new electric outlet can be measured and described in a way that can be replicated by others, security generally (and cybersecurity, in particular) remains more art than science.

For example, we can and do understand that a new

**Passengers** use Global Entry kiosks at an international airport (James Tourtellotte / Public Domain)

intrusion detection system improves the security of an enterprise, but we cannot say with any confidence by how much it does so. Likewise, we can and do say that any deployment of a new system — say, an upgrade to an accounting package — will bring with it unknown or previously nonexistent vulnerabilities that might manifest themselves. And yet again, we cannot with confidence measure the change.

Grappling with this challenge and others like it is fundamental to the maturation of an enterprise cybersecurity model. When a corporate board faces a security investment decision, it cannot rationally decide how to proceed without some concrete ability to measure the costs and benefits of its actions, nor can it choose between competing investments if the comparative value of those investments cannot be measured. Likewise, when governments choose to invest public resources in a security measure or otherwise regulate private-sector activities, they must do so with as much information as possible.

## MEASURING PRIVACY

The same problems exist, to an even greater degree, when we turn to the question of measuring privacy.

To begin, privacy seems to be inherently less capable of measurement than security. At least in the security context, we can imagine some concepts that lead to neutral, objective metrics of success. Security might, for example, be measured by lives saved, intrusions prevented, crime reduced, or even malicious actors captured. We might even decide, in some contexts, that we care less about the harm caused by the security breach than we do about recovery from the breach, and thus choose a security metric based on how quickly we can overcome the effects of a security failure. None of these measurements would be perfect, but in theory, we might begin the discussion.

In the case of privacy, we are more skeptical of the existence of neutral, objective metrics. This is, in part, because privacy is in many ways a hedonic value, which is to say that different individuals assess it in varying ways. Some would gladly trade personal data privacy for increased physical privacy, as evidenced by the fact that many participate in Global Entry and the Transportation Security Administration's (TSA) Pre-Check program, which allows the government to screen their data for threat indicators in exchange for an easier physical screening experience when traveling. Others, however, might make the contrary choice, preferring data privacy while accepting an increased compromise of their physical privacy. We know of no way of determining which one is "right" and which is "wrong" in that assessment.

Even more problematically, we might not only disagree as to which privacy value is superior, we might also disagree on the intensity of our preference. If one person feels strongly about his choice and another person is indifferent to the matter, that makes the privacy measurement difficult. In short, because people experience privacy very differently, it is much harder to imagine a uniform, generally agreed-upon privacy metric.

One way we deal with this uncertainty now is to hide it behind ambiguous phrases that hint at metrics without any actually existing. Regulators in Europe, for example, ask whether privacy disclosures are "proportionate" or whether systems of privacy protection are "adequate." In some ways this is understandable — they are trying to give expression to the inexpressible. But in the end, this phraseology is little more than the law of the Chancellor's foot, disguising decisionmaker-based policy preferences as some objective criteria.[3]

Another way to deal with the privacy metrics problem is to deny that it is relevant to a policy discussion. The question of metrics, and efforts to answer it, are only of interest to those who begin from the first principle that neither privacy nor security are absolutes. There are some who disagree — notably those who think privacy is an inherent human right that cannot be extinguished or traded away. For them, this entire exercise is an affront.

But this position is surely untenable. Protecting privacy requires acknowledging that both privacy and security are instrumental values and not absolutes. To be sure, this makes policymaking far more difficult. It means, for example, that we need to look at privacy as a construct used to protect other important values — things like autonomy, self-determination, democracy, and liberty of conscience — and try to be clear about connections between them. But the fact that an exercise is difficult does not mean the effort should not be made.[4]

## THE SOLUTION

So where does that leave us? Is it impossible to measure privacy or security at all? Is the tradeoff paradigm flawed at the foundation because it demands that which does not yet exist and, worse yet, cannot reasonably be thought to ever be feasible?

One certainly hopes not, for there is another failure mode that is possible — the opposite of valuing privacy as an absolute: the belief that if privacy cannot reasonably be measured, then its value may be assessed as nonexistent. When combined with our security impulse, this lack of a privacy metric can drive us to disregarding privacy altogether. And so, as a result, the pendulum swings — from 9/11 to Snowden and then, perhaps, back again. This sort of schizophrenia leads to bad policy.

How, then, do we square the circle and measure privacy? The answer likely lies in the concept of consequence rather than intrusion.[5] To be more explicit, the measure of privacy — if we can develop one at all — depends on tying privacy intrusions to real-world consequences: insurance denied, job applications rejected, or searches conducted. That sort of variegated, diffuse concept of privacy harm is assuredly difficult, but the lack of any attempt to measure privacy at all is even more problematic.

Because the problem of measuring security and privacy is at the core of sound policy, law, and business judgment, it is critical to get right. The absence of agreed-upon metrics to assess either means that many companies and agencies lack a comprehensive way to measure concrete improvements in their security or privacy protection. To that end, the U.S. government needs to launch an initiative to build a consensus around how to fill that gap. Without measurement, we are doing nothing but expressing our opinions and preferences — and in a time of enhanced threats, constrained resources, and changing notions of privacy, that simply is not an adequate response. In the end, we really must know just how much a "privacy" weighs.

[1] Benjamin Wittes, "What Ben Franklin Really Said," Lawfare Blog, July 15, 2011, <https://www.lawfareblog.com/what-ben-franklin-really-said>.

[2] From The Chertoff Group, The Ground Truth About Encryption And The Consequences of Extraordinary Access, 2016, <https://cdn2.hubspot.net/hubfs/3821841/docs/238024-282765.groundtruth.pdf>.

[3] The law of the Chancellor's foot refers to a law that depends exclusively on the predilections and tendencies of the decision-maker. As John Selden put it in the 17th century, "Tis all one as if they should make the standard for the measure we call a foot, a Chancellor's foot; what an uncertain measure would this be? One Chancellor has a long foot, another a short foot, a third an indifferent foot: 'tis the same thing in a Chancellor's conscience." J. Selden, "Table Talk," quoted in Michael Evans, Ian Jack, eds., Sources of English Legal and Constitutional History, at 223–24 (Sydney: Butterworths 1984).

[4] Paul Rosenzweig, "Whither privacy?" Surveillance & Society, 10, 344-47 (2012), <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/whither/whither>.

[5] Paul Rosenzweig, "Privacy as a Utilitarian Value," Lawfare Blog (November 12, 2014), <https://www.lawfareblog.com/privacy-utilitarian-value>.

Paul Rosenzweig

Paul Rosenzweig is a Senior Fellow at the R Street Institute and a Professorial Lecturer in Law at George Washington University. He served as the Deputy Assistant Secretary for Policy at the Department of Homeland Security from 2005 to 2009. He is also the Principal at Red Branch Consulting.

JCDecaux
False news is not your friends.
News United posted a photo
Monday at 8:21 PM
10 Comments
Like
Comment
Share
Facebook is changing so you see more from your friends and less of the stuff that gets in the way.

> We’re seeing more and more local newspapers and media outlets go under, and these local outlets are kind of the connective tissue between people and their governments

**Facebook** advertisement against misinformation
(Kevin Tao / CC BY 4.0)

# Learning from Russia's Influence Campaigns in Eastern Europe

## A Conversation with Nina Jankowicz

Interviewed by FSR Staff

**Fletcher Security Review:** Thank you for taking the time to speak with us. Can you begin by telling me a bit about the work you're doing right now?

**Nina Jankowicz:** Sure. I am working on a book that tracks Russian influence in Central and Eastern Europe over the past decade. But rather than kind of looking at tactics and techniques, which we know a lot about already, it's looking at responses, which I think the West has yet to really observe. We tend to think that this is the first time this has ever happened to and we need to reinvent the wheel and our response. And I actually think there's a lot to learn from countries like Estonia and the Czech Republic in what they've done right, and what they've done wrong.

**FSR:** Can you talk a bit about what Estonia and the Czech Republic have done right and wrong?

**NJ:** Estonia, as you might know, has a large ethnic Russian population and dealt with this Bronze Soldier crisis in 2007 where the government wanted to move, and did move, a Soviet statue from the center of capital talent into the outskirts, which isn't saying much because Tallinn is quite small. But the Russian government used this and the marginalization of the ethnic Russian population in order to foment unrest. And this is a typical tactic that the Russians use: preexisting societal fissures that create distrust in institutions and dismay among the general population. So there were protests.

There was also a cyber attack attributed to Russia. It shut down a lot of banks, media outlets, and some government websites. It was what I call "Disinformation: beta version" because they didn't have much social media back then. So fake news and disinformation are traveling via normal media outlets because the Russian population was kind of marginalized and only had these Russian language outlets. All of that background is to say that the government in Estonia, rather than focusing on a kinetic response directly toward Russia, which it obviously did as well, invested in people and trying to repair that fissure between ethnic Estonians and ethnic Russians in society: investing in education, investing in media, investing in people to people contact. Since the annexation of Crimea there was some nervousness about what might happen with the concentrated Russian areas in Estonia.

There's one town called Narva that's 95 percent Russian. It's right on the border. The new government that came in was really investing in that. Since 2014 the new

TÕNISMÄGI WAR GRAVE ARCHEOLOGICAL
EXCAVATION AND IDENTIFICATION SITE
THANK YOU

**Protests** against the removal of the Bronze Soldier of Tallinn (Leena Hietanen / CC BY SA 4.0)

**President of Estonia** Kersti Kaljulaid (center left) meets with President of Russia Vladimir Putin (center right) (The Russian Presidential Press and Information Office / CC BY 4.0)

president, Kersti Kaljulaid, has actually done a little sabbatical where she moves her presidential administration to Narva and there's a lot of investment in the town, and for the first time people are kind of feeling like they matter when they've been neglected to a strong degree. So, a lot of the responses that I advocate for in my work are based on people. These problems that exist can be exploited by any bad actor, whether it's Russia, Iran, China, Bangladesh, or Venezuela, as we've seen recently.

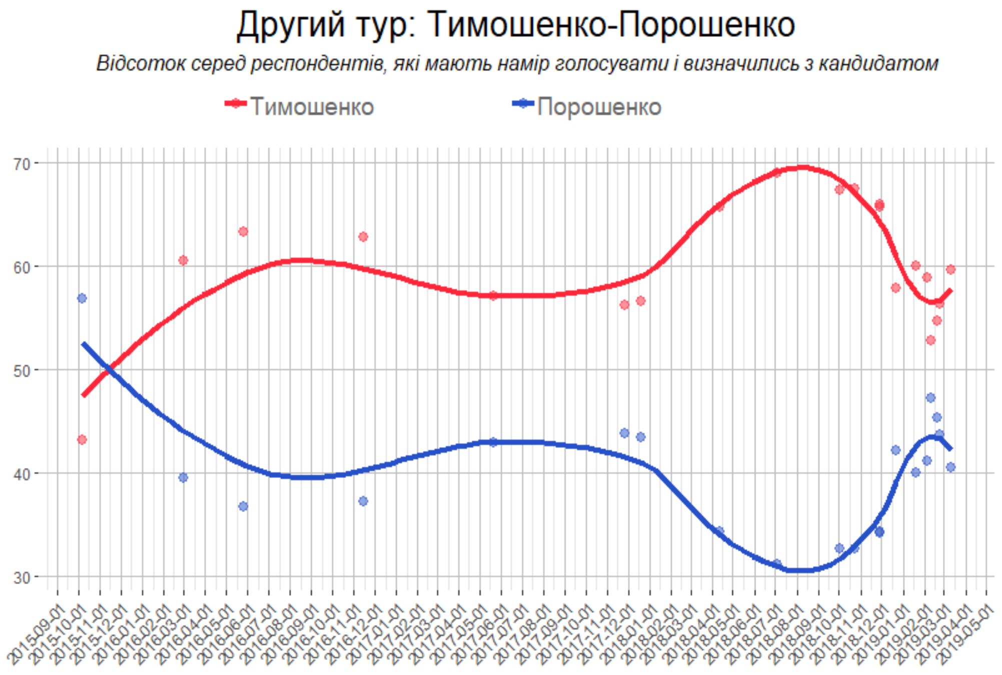
It's one thing to say: we need to have good governance. You can't exactly legislate that, but you educate people. You can also invest more in civics because a lot of the disinformation that we see has legs because people don't understand how the government works. If they understood what it was actually like inside a lot of these government agencies or even at their local level, I think a lot of this stuff would seem a lot less intriguing.

I think that sort of thing is a wider spread than most people recognize, and part of that is the atrophying local media environment as well. We're seeing more and more local newspapers and media outlets go under, and these local outlets are kind of the connective tissue between people and their governments. So those are the things that are exploited and those are the things that I think we need to focus on repairing.

**FSR:** That's fascinating.  I also read that you've managed democracy programs in places like Belarus. Can you talk a bit about your experiences there?

**NJ:** The National Democratic Institute has been around for about 35 years. They manage democracy assistance programs all over the world but got their start kind of in the end of the Soviet-era in Eurasia and Eastern Europe. I worked on Russia and Belarus, and a lot of the assistance that we did with activists in those countries is centered around political parties: party building, party communications. We did some election observation trainings and  skills building as well. We designed programs that activists could come to and work on how to conduct voter outreach or how to do petitions on how to make civil initiatives happen in their communities.

Belarus, in particular, is really interesting because of its geopolitical position. It's kind of like a pendulum that swings back and forth between Russia and the West. When it's not getting what it wants from Putin, it comes to the west and the West is like, *ah, finally this is our chance to make a difference in Belarus*. But inevitably something else happens that brings it back to Putin. So



**2019 Ukrainian Presidential Election's** **s**econd round. Tymoshenko (red) vs Poroshenko (blue) (Kosandr / CC BY-SA 4.0)

we've seen that happen. The most recent one before this was in 2010, and we're seeing it happen again. This is the third such pendulum swing, and they often end in a crackdown on democratic activists.

This one has been brought about by the fact that Lukashenko doesn't like that Putin has designs on Belarus. There's already Russian military bases in Belarus, and there's been some talk of the “Putinization” of Belarus. Lukashenko likes that. If you read any of these hot takes in any of the foreign policy type establishment magazines that are writing about the new thaw Belarus, it might look like a thaw, but it's not going to last one way or another. That's why Lukashenko has been in power for 30 years. And human rights and civil rights in Belarus are still really quite poor. So we might look and say, *you know, he's trying to cozy up to us*, but we should look at it at face value and understand that this is often how things work there.

**FSR:** What do you think Russia’s influence is going to be over the upcoming elections in the Ukraine?

**NJ:** Well, Ukraine has always been the kind of laboratory or petri dish for all of these techniques. We saw some Sputnik-related pages get taken down recently where they were posing as local news outlets. They were looking like local news and talking about these issues and then linking back to Sputnik content. This is where they create trust around real issues, then try to get people to turn out, whether that's signing a petition or changing their profile picture on Facebook or coming out to an event like a protest.

Ukrainians have a lot of apathy toward their government right now and toward all of the candidates. Polling is really hard in Ukraine, but the last I saw, around 20 percent of voters are still totally undecided, and the election is in less than two months. There’s only one new face, and then everybody else is a known quantity to Ukrainians. Ukrainians have a bit of savior complex where they want somebody new to fix things all the time. Certainly Poroshenko and Tymoshenko, the two other leading candidates, are quite tainted for various reasons, but they both have decently strong support. I mean it's still under 20 percent. So all this to say it wouldn't be hard to continue to inspire that apathy.

If you look at the posts that Facebook took down from Sputnik, they gave a couple of examples.

One of them was about the quality of water in that particular town. One of them was they had some NATO related posts, which isn't really a firebrand issue in Ukraine, but it's a little bit divisive. So again, real issues, real complaints, but things that if just kind of tweaked a little bit could keep people home or have them vote for somebody that may not be as qualified for the post.

Facebook has said that is not going to allow political advertising to be bought from outside of Ukraine, but I don't think that will be hard to fake. I'm going to be looking for new things that they're Kremlin might be able to use in 2020 that they're trying out in Ukraine. But so far we've, I don't think we've seen too much of that.

**FSR:** What aspects do you see of the Russia disinformation campaign against the US in particular that are the most dangerous or insidious?

**NJ:** I think it is deceptively simple. I think a lot of people have focused rightly on protecting election infrastructure. We've seen a lot about the need to re-up our cyber fences around voter rolls and election commissions at the state level. And we need to make sure that the campaigns have good digital hygiene. And that's all really good and really important, especially on a campaign level because that was a bit difficult during 2016. But those are easy things to do. The much more difficult fixes are the ones that I was talking about before where we need to invest in people's greater understanding of the problem.

The way that Russia exploits that is two-fold. They use these preexisting fishers in society through positive campaigns, that are grounded in kernels of truth, if not totally true, but with like a crazy spin on it. This makes it really difficult for social media platforms to say, *this is fake, let's fact check those, and then if it's fake, we'll take it off the platform.* Because it's not necessarily fake news - I think it comes down to this lack of critical thought that a lot of people have based on online news consumption.

So there's a lot of focus and part of this is because of the Trump administration, the focus that they're putting on it, and the lack of political will to address these things. But there's a lot of focus on election infrastructure. Just yesterday (Feb. 5, 2019), the DHS and DOJ put out a statement about the report that they're delivering to the president that says that there was no tampering with voter rolls or votes during the midterms, which is true, but we know for a fact there was an ongoing online influence campaign. There probably still are accounts that are active on both Twitter and Facebook, probably more on these crazy alt-right websites, certainly on Reddit we've seen that they're continuing to represent themselves as Americans and influence U.S. discourse.

That's the type of thing that's a lot more nefarious, a lot more insidious, and really hard to put a finger on. I don't think it's Russia's goal to actually go in and change voter tallies. I think they want to inspire doubt in the system. So even by DOJ and DHS putting that statement out there that says they didn't do it *this* time is feeding into the Russian goal because what Russia wants people to think is, *my vote might get changed, my vote doesn't matter as much, so I'm not going to go out to vote.* It's this very complex voter suppression psychological thing. All Putin has to do is rattle the door knob of one voter file once for us to have that doubt in the system. And that's more dangerous for democracy then than any actual vote tampering that they could do.

**FSR:** So they don't want to do the dirty work themselves. They want to inspire us to do it ourselves.

**NJ:** Absolutely. Whether you're talking about disinformation or cyber activities, that's exactly what Russia wants to do. And also it helps them have plausible deniability. It's like, *oh no, we didn't do it, are you really going to try to slap some sanctions on us for rattling the door handle to your voter roll?*

**FSR:** What do you think we can expect in the 2020 elections?

**NJ:** I get this question a lot and I think there's no reason to expect anything different. We've not seen enough of a change from the platforms, the government, or the public, to expect that any bad actor will really change their tactics. In fact, we've seen the Russian playbook has been laid bare for other bad actors, and we've seen it replicated across the countries that I named before. This is cheap. This is effective. They probably still have thousands of accounts working on their behalf.

Russia and others are also finding out ways to get around them. I think we'll see more of the same, except a bit less brazen. We're not going to see ads paid for in Rubles, or traffic coming from Russian IP addresses. It's going to be masked via VPN and they're going find other ways to get around it and pay for it, whether that's through explicit cooperation with sites or fringe entities that support the Russian mission. In terms of the actual tactics, there's no reason to think that they'll change.

Fake accounts are not your friends.
James Anderson posted a photo
Tuesday at 5:04 PM
Seun Shobande and 61 others
7 Comments
Like
Comment
Share
Facebook is changing

**Facebook** advertisement against fake accounts (Kevin Tao / CC BY 4.0)

And I know that's not a super sexy answer, but it's the truth.

**FSR:** Are there other actors that you think are going to try to imitate Russia?

**NJ:** Well, we've already seen sites from Venezuela and Iran trying to do the same. China really hasn't gotten into this as much because they've got their own stuff at home, but I am sure they are creating their own textbook for these opportunities to exploit when they need to. I would also add that these tactics are being mimicked by homegrown actors as well. We're seeing it. In fact, I wrote a story about a candidate for Senate in Massachusetts who was running against Elizabeth Warren. You might've seen his crazy ads earlier in the year—Shiva Ayyadurai. He had an astroturfing operation that I can't directly attribute it to his campaign, but I alerted Facebook to these accounts, which were clearly fake, they had fake profile pictures. They all posted the same things at the same times across a variety of anti-Warren and pro-Trump Facebook groups that were in favor of Shiva Ayyadurai. They're all added to groups by each other or by people associated with the campaign. So I don't know that this candidate said, *go create these accounts*, but someone who supported him was doing this.

That's the sort of thing that we're going to see a lot on both sides of the political aisle. And what I want to see is politicians standing up against it and saying, *all members of our party are going to adhere to these rules and we're not going to engage in the same type of behavior that bad foreign actors do.* Because otherwise, we're just totally screwed.

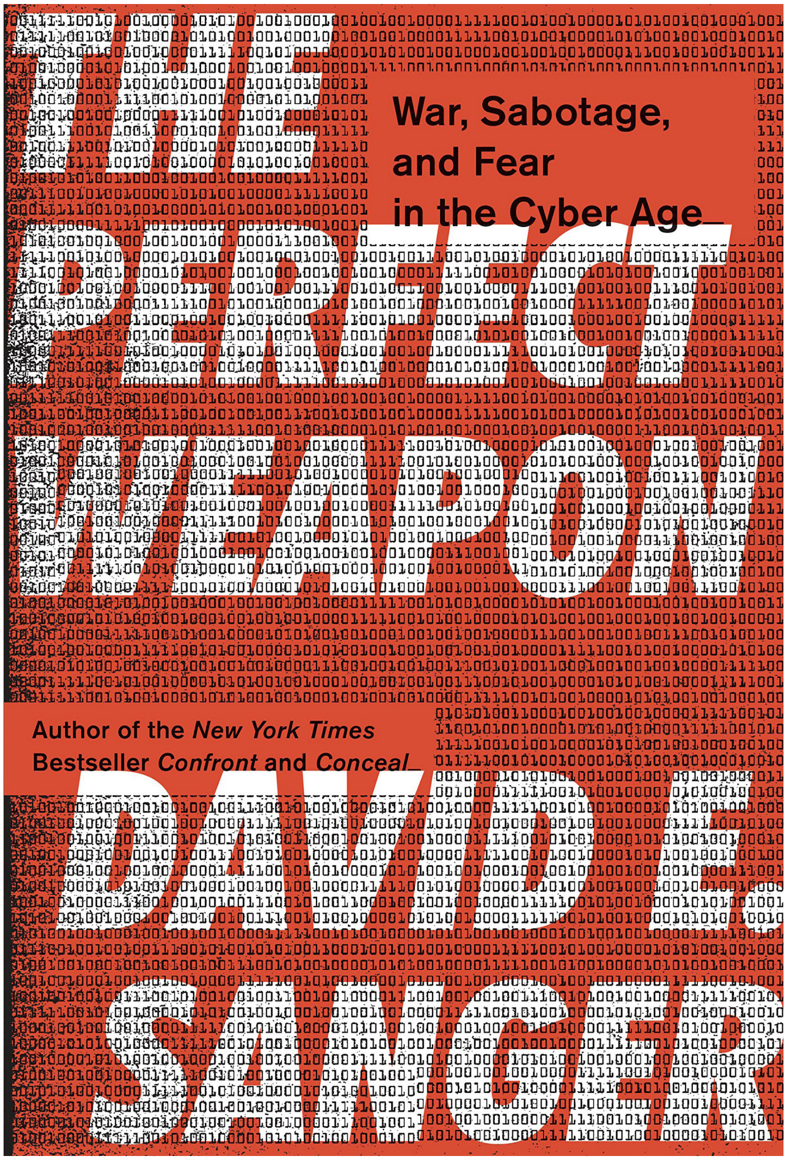
## Nina Jankowicz

Nina Jankowicz is writing a book on the evolution of Russian influence campaigns in Eastern Europe. She has previously worked advising the Ukranian government on communication and managed democracy assistance programs for Russia and Belarus. She is currently a Global Fellow at the Woodrow Wilson International Center for Scholars' Kennan Institute and has previously served as a Fulbright-Clinton Public Policy Fellow.

# *The Perfect Weapon*

## *War, Sabotage, and Fear in the Cyber Age* by David E. Sanger

A Book Review by Travis Frederick


War, Sabotage, and Fear in the Cyber Age_
Author of the *New York Times* Bestseller *Confront* and *Conceal_*

"No modern military can live without cyber capabilities, just as no nation could imagine, after 1918, living without airpower."

In *The Perfect Weapon,* David Sanger argues that the nature of global power itself is undergoing dramatic changes, brought about by the proliferation of highly advanced cyber capabilities. Today, internet access is nearly ubiquitous, the cost of entry is low, and, particularly in the domain of cyberwarfare, there is one fundamental fact: offensive capabilities have critically outpaced cyber defenses. A weak and impoverished nation like North Korea can hold large swaths of public and private infrastructure in America at risk, steal military OpPlans, and pilfer millions of dollars from foreign banks. A Kremlin reeling from sanctions, low oil prices, and historically low public trust is able to threaten the very foundations of American democracy through targeted social media campaigns and hacking and leaking the emails of a major political party. But while the offensive advantage has given weaker powers greater capacity to pursue their geopolitical objectives, U.S. leadership has found that their response options have not similarly benefitted. America's offensive cyber prowess so exceeds its own defensive capabilities that officials often hesitate to strike back for fear of establishing norms of retaliation against vulnerable infrastructure or inciting unintended escalation. Sanger argues that without an open public debate among government policy makers, military planners, and academics to coordinate a grand strategy, the United States will be forced to accept a world of constant cyberattacks, limited response options, and the greater risk of capitulating to foreign coercion.

Throughout Sanger's numerous interviews in *The Perfect Weapon,* there is an unmistakable tension present in the cyber security views of public officials, intelligence agencies, and private companies. How should they respond to cyberattacks and known defense vulnerabilities? In response to Russian interference in the 2016 U.S. presidential election, some officials advocated retaliation by punishing Russian President Vladimir Putin personally, freezing oligarch money around the world, or by conducting an in-kind hack and leak operation against the Russians. Yet, the most common U.S. response to attacks has been either low-cost symbolic action, or to secure defenses and not respond at all. One Obama-era official noted the reticence to even publicly attribute known attackers because, "Once you say who committed an attack, the next question is, so what are you going to do about it?" Intelligence officials have encouraged this government silence, arguing that by attributing an attack, states reveal both their capacity to monitor their own networks as well as adversary systems. Likewise, they argue that public acknowledgement of one's own offensive cyber capabilities undermines previously secret advantages their forces may have had. Private companies have pushed back against this silence, arguing that the government bears the responsibility to publicly reveal potential attacks or network vulnerabilities once it has found them. Reflecting a lack of confidence in government responses, some tech giants have taken to "active defense"—hacking back. So, how should the United States respond to cyberattacks and known defense vulnerabilities?

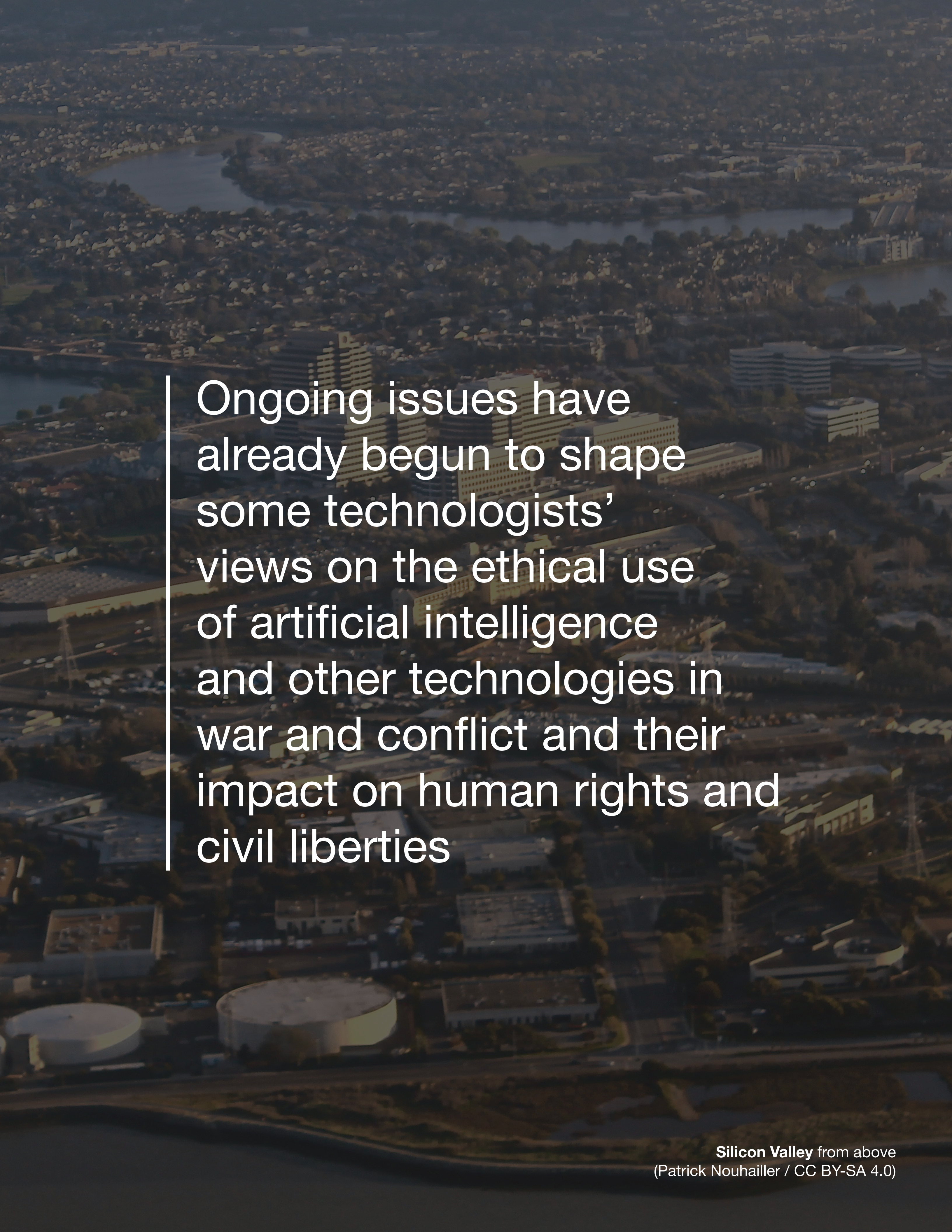
The primary argument of *The Perfect* W*eapon* is that despite years of spending billions of dollars on new offensive and defensive cyber capabilities, the United States has failed to create a successful deterrent against cyberattacks. By first acknowledging the folly of going on the offense without a good defense, Sanger advocates for establishing a policy of deterrence by denial. He goes on to provide a set of policy recommendations based on securing U.S. defenses and establishing international norms against cyberattacks. He believes that these two pillars of cyber policy, namely a strong defense and international norms of non-aggression, will most effectively support U.S. national security in the coming decades. This will require a Manhattan Project-like commitment to secure the most critical infrastructure and a set playbook for responding to attacks. This playbook requires that the U.S. enhance its capabilities to attribute attacks and make calling out adversaries the standard response to any and all cyber aggression.

One critique of Sanger's emphasis on deterrence by denial is that it does not introduce costs sufficient to change the calculations of malicious actors. Even with an effort on the scale of the Manhattan Project to shore up U.S. defenses combined with calling out adversaries, it is implausible that the costs of an adversary's failed attempts to penetrate critical networks or public shaming will ever meet the threshold to successfully deter further attacks. During an interview with the author of this review, David Sanger acknowledged the limitations and tradeoffs of a primarily deterrence-by-denial approach. However, he also argued that policy options are constrained by the reflexive secrecy of the national security establishment regarding offensive cyber capabilities, which has effectively undermined any cost the United States may hope to instill in the minds of its adversaries. In order to create any kind of cyber deterrent or engage in any negotiation of limits in cyberspace, the United States is going to have to be willing to acknowledge some of its own capabilities. By pushing back on some of the system's reflexive secrecy, Sanger argues, the United States can acknowledge some of what it can do in order to threaten adversaries, and importantly, what it will not do in order to begin establishing global norms in cyber conduct. Through hardened defense, norms of non-aggression, and progress towards eventual cyber arms control, Sanger hopes that one day a strategic stability will be reached where the world will be able to reap the full benefits of a technological society without being held captive by burgeoning cyber vulnerabilities.

Truly compelling for security scholars and casual readers alike, *The Perfect Weapon* provides a fast-paced, detailed history of cyberattacks. David Sanger adroitly illustrates the central dilemmas of cyber policy and the tensions among its key U.S. actors, all while maintaining a sense of immediate concern for the immense dangers posed by cyber warfare. This book has a breadth and depth that will engage casual readers and urge professors to update their course syllabi with several new chapters.

## Travis Frederick

Travis Frederick is a Ph.D. candidate in security studies at Princeton University and a graduate researcher in Princeton's Socio-Cognitive Processes Lab. His research interests include Russian security policy, U.S.-Russia relations, and the psychology of threat perception. He is a Graduate Fellow at the Center for International Security Studies and has previously worked at OSD Policy, U.S. State Department, and GTRI.



> Ongoing issues have already begun to shape some technologists’ views on the ethical use of artificial intelligence and other technologies in war and conflict and their impact on human rights and civil liberties

**Silicon Valley** from above
(Patrick Nouhailler / CC BY-SA 4.0)

# A Healthier Way for the Security Community to Partner with Tech Companies

Dr. Douglas Yeung

Digital data captured from social media, cell phones, and other online activity has become an invaluable asset for security purposes. Online mapping or cell-phone location information can be used to collect intelligence on population movement, or to provide situational awareness in disasters or violent incidents. Social-media postings may be used to vet potential immigrants and job applicants, or to identify potential recruits who may be likely to join the military.

However, breakdowns in relationships between the tech industry and would-be consumers of technology's handiwork could imperil the ability of security stakeholders to use this data. Ongoing issues have already begun to shape some technologists' views on the ethical use of artificial intelligence and other technologies in war and conflict and their impact on human rights and civil liberties. It isn't difficult to imagine a series of future incidents further souring collaboration between technologists and security stakeholders.

In contrast to its reluctance over security matters, the tech industry has been a willing partner for government agencies and communities that promote health and wellbeing—topics that present less of an ethical challenge. Although it may not be immediately apparent, wellbeing and security have much in common. Could the security community take a page from wellbeing efforts to improve their collaboration with the tech industry?

## BIG TECH HOLDS MOST OF THE CARDS

Maintaining data-sharing partnerships with the tech sector is critical to ensuring that security interests can access timely, representative, and complete data sets; build and operate robust data transfer pipelines; and maintain reliable data storage and backups. Properly interpreting data requires highly trained analysts and organizational support, analytic tools, and knowledge-sharing policies and protocols. Data must also be distributed to those who need it most—intelligence analysts, military commanders, and senior decision makers—and safeguarded against theft or loss. As with any security mission, interrupting the supply chain (in this case, digital data, its supporting infrastructure, and access to tools and trained personnel) can threaten the mission's success.

Given the market dominance of a few big companies, such as Amazon, Facebook, and Google, these digital assets and capabilities likely cannot be acquired through other channels. Social-media companies tightly control data access, while big data-management and analytic capabilities often reside in cloud-computing companies. As a result, tech companies have become critical security partners for governments and other stakeholders. As with allied nation-states or international coalitions, maintaining working relationships and cooperation is essential for continued data flows.

## LACK OF TRUST IMPERILS TECH-SECURITY COLLABORATION

Perhaps the key challenge to these partnerships is a loss of trust resulting from a perceived mismatch in institutional goals between government security agencies and the tech companies on which these agencies have come to depend. Vocal tech workers have taken actions to block their employers from cooperating with government agencies or working on projects that the workers find objectionable. In 2013, leaks about the National Security Agency's (NSA) alleged data-collection activities strained relationships between the NSA and tech companies as well as members of Congress, foreign government leaders, and the public. After criticism from the public and their own employees, tech companies such as Yahoo, Google, Verizon, and Apple increased security measures, called for surveillance reform in a joint open letter expressing some distrust of the government, and released "transparency reports" that detailed the government's requests for information and how the companies responded (e.g., what type of information was shared).

More recently, Microsoft employees demanded that the company stop working with Immigration and Customs Enforcement to protest family separations at the U.S.-Mexico border.[1] Google employees signed a petition and some even resigned in protest over Google's work with the Department of Defense on artificial-intelligence capabilities for drones.[2] Amazon employees, citing family separations and government surveillance, objected to selling the company's facial-recognition software to law-enforcement agencies.[3] These companies have ended some security-related projects and may be wary of ongoing or future government cooperation on security matters.

Tech companies have taken other concrete actions such as hardening security protocols to impede law enforcement or intelligence agencies from intercepting communications, and either canceling or declining to bid on government defense contracts.

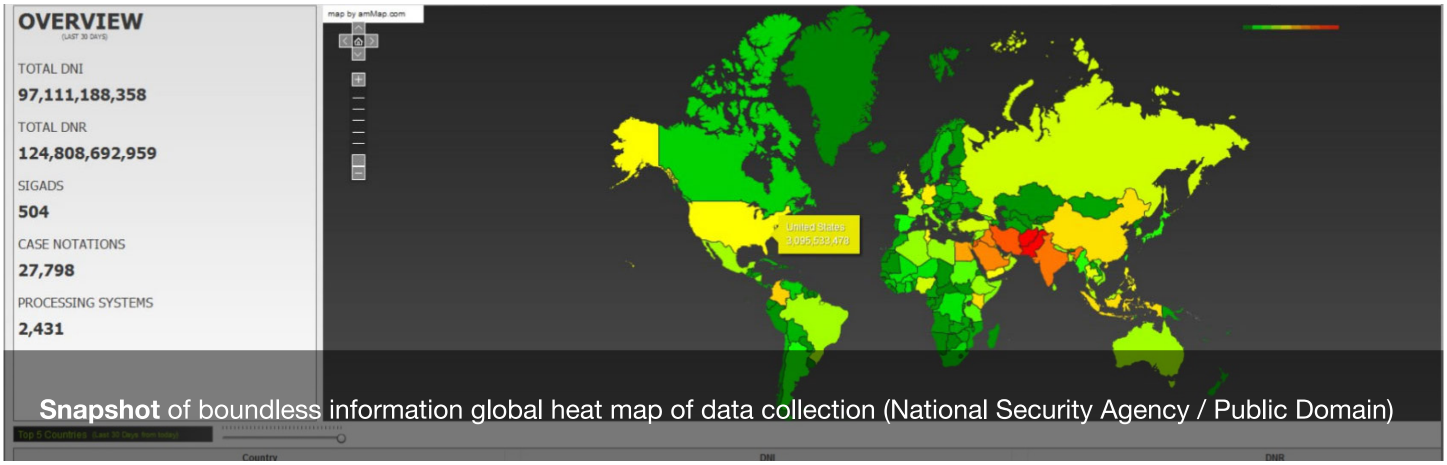
## ADVANCING SECURITY THROUGH WELLBEING

There is another path to advancing security—one that piggybacks on the burgeoning public-private cooperation around civic wellbeing. Governments at all levels and in communities around the world are leading initiatives to improve collective wellbeing though the use of digital data. These efforts emphasize measuring how local conditions, policies, and programs influence quality of life, and promoting those that have the largest positive impact. The institutions at the forefront of these efforts have worked to ensure they are making the best use of technology-derived insights to address intractable societal problems.

These collaborations benefit from the tech industry's perceptions of their government partners. In contrast to security-related collaborations, the tech industry appears to hold a more positive view of the government's motivations when the goal is society's wellbeing.

Two examples illustrate how collaborations between local governments, tech companies, and other civic organizations have succeeded. Air Louisville, for instance, is a community partnership program that began in 2012 to provide local government with information about air quality in Jefferson County from sensors fitted to residents' asthma inhalers.[4] This data-driven collaboration between philanthropic funders, public agencies, and private tech companies mapped environmental conditions and corresponding health risks, and used that information to identify mitigating actions, such as rerouting trucks away from high-risk areas.

The City of Santa Monica's Wellbeing Project sought to go beyond traditional (e.g., economic) performance measures to measure government's impact on the wellbeing of its residents. Santa Monica's Wellbeing Index has engaged multiple partners to collect and make use of data and emerging technologies to provide a shared understanding of community strengths and needs. For example, the RAND Corporation, headquartered in Santa Monica, has worked to help Santa Monica measure civic wellbeing, partly through analyzing social-media data, and embed that information into policymaking. Santa Monica also partnered with RAND, Fitbit, and Fitabase, a research platform for health tools, to observe indicators related to physical activity or other factors of wellbeing. With more information about residents' health, Santa Monica plans to improve city planning and investments, and design programs and policies to improve resident wellbeing. In both cases, the city's


OVERVIEW
(LAST 30 DAYS)

TOTAL DNI
97,111,188,358

TOTAL DNR
124,808,692,959

SIGADS
504

CASE NOTATIONS
27,798

PROCESSING SYSTEMS
2,431

**Snapshot** of boundless information global heat map of data collection (National Security Agency / Public Domain) tech partners likely joined the effort in part to advance wearables and other tech products that are positioned to play a role in digital health, telemedicine, and precision medicine.

## WELLBEING AND SECURITY ARE COMPLEMENTARY DOMAINS

While the similarities may not be immediately apparent, wellbeing and security are, in fact, complementary concepts. Both involve societal institutions striving to ensure the safety and welfare of their citizens. Additionally, both include the notion of collective benefit, or that collective actions may not offer direct benefits to an individual or group but should be undertaken to advance the mutual interests of an entire community. Examples of this principle of shared responsibility for security include mutual defense treaties, security alliances and coalitions, and, for wellbeing, international bodies convened to tackle global health crises.

Similar to security efforts, wellbeing initiatives focus on understanding broad factors and upstream drivers that influence the state and stability of an entire community or group. Both domains attempt to build resilience to buffer the population against natural disasters, infrastructure catastrophes, terrorist attacks, or war. Programs and interventions in each domain create conditions that can fulfill more fundamental requirements for economic and physical security (e.g., physical infrastructure) as well as higher-order goals (e.g., public optimism). For instance, a foundational aspect of wellbeing is developing healthy attitudes and behaviors as well as a sense of community, each of which starts with creating shared values among community members.[5] Relatedly, counterinsurgency or other military campaigns may seek to “win hearts and minds,” acknowledging the importance of gaining a population’s trust.

Economic opportunity, which includes the availability of jobs, businesses, and affordable housing, is a critical component of both wellbeing and security because it provides people with financial security and stability. Concerns about financial security and a lack of prospects can hollow out a community, as young people move away to seek jobs, leaving less-mobile individuals behind and without support. Similarly, refugees and asylum seekers in search of a better life due to economic or safety concerns are often seen as a security threat or an economic burden. Yet research suggests that refugees and other migrants actually provide economic benefit to a region.[6] Wellbeing or security efforts that address economic vulnerability or humanitarian crises in potential migrants’ home countries may slow their outflux, as improved community conditions allow people to thrive in place.

Similarly, wealth inequality presents a serious threat to both global stability and wellbeing. Prominent individuals such as former President Barack Obama, billionaire investor Warren Buffett, and Facebook CEO Mark Zuckerberg have all decried the detrimental economic impact of income inequality.[7] Some community wellbeing stakeholders have made addressing inequality an explicit goal, or even their central mission.[8] Increasingly, inequality is also seen as a multidimensional security challenge, such as by fueling populist sentiment.[9] Governments routinely undertake a wide range of security assistance, economic development, and other foreign aid programs, each with differing priorities and stated goals. Collectively, these programs could be viewed through the lens of addressing inequality.

Finally, population diversity benefits both wellbeing and security. It adds richness to societies, and it can improve creativity and performance in smaller groups. Military recruiting leaders, for example, emphasize the importance of creating a diverse mix within the armed forces that reflects the breadth of the general population.

## HOW COULD A WELLBEING APPROACH BRIDGE THE TECH-MILITARY DIVIDE?

Given these commonalities, the question for security stakeholders is this: to what extent could they use digital data and other emerging technologies to better understand and monitor the health and security of communities, and then look to solve problems that are central to societal wellbeing? Digital data from tech-sector partnerships support several key functions for wellbeing that may also fulfill security requirements. For example, social-media content is useful to track public sentiment and to estimate political will. Geolocation data can provide information to allocate resources and position infrastructure. These and other forms of digital data are useful to provide situational awareness in preparation for disasters or unexpected events, and to inform forecasts and predict trends.

The U.S. government has begun to address this question

**CSO of Headspace** Dr. Megan Jones Bell (center) speaks at HealthConf (Web Summit / CC BY 4.0)

by increasing its outreach to and engagement with the tech community. Attempting to head off the potential loss of access to critical technologies, U.S. national security and intelligence agencies have established several Silicon Valley outposts (e.g., In-Q-Tel, Defense Innovation Unit) to increase their presence and build relationships in the tech community. Additionally, direct engagement on contentious topics could send a more powerful signal of openness. For instance, the mission of the Department of Defense's newly created Joint Artificial Intelligence Center emphasizes engaging artificial-intelligence researchers and developers on tech ethics and civil liberties.

Another potential avenue to bridging civil-military divides would be to explore how governments and tech partners have successfully collaborated on wellbeing in the past. How were tech and wellbeing collaborations forged, and what motivated tech companies' leaders and employees to join them? Tech companies may find it beneficial to signal that they are working productively to improve the wellbeing of a community, for example. As evidence, consider the existence of several wellbeing-focused corporate arms of tech companies, such as Google's Sidewalk Labs, Headspace Health, Uber Movement, and Airbnb Citizen. Tech companies, in contrast, may wish to signal to internal and external audiences that they are not cooperating on controversial uses of digital data. This may suggest that the security community should deliberately consider how potential collaborations or uses of digital data might be perceived by the public and the tech industry. It may also suggest that security stakeholders reframe or refocus their efforts on issues like inequality that cut across wellbeing and security. In this manner, tech and wellbeing could be a model for how to use tech productively to improve wellbeing and security, and for a less controversial path to tackling fraught or challenging issues.

## CONCLUSION

Developing and harnessing technological innovation is an essential step on the path to advancing security. Whereas technological innovation was once limited to the nation-state, today it often resides in private companies across the world. Debates have erupted over the appropriate use of this technology, and these disagreements threaten the continued ability of governments and other security stakeholders to develop advanced capabilities. On the other hand, attracted by the potential for digital data to inform policymaking and improve decision making, a growing number of governments and nongovernmental institutions have successfully partnered with the private sector to analyze this data as a means of increasing societal wellbeing.

Existing efforts to promote community health and wellbeing have included stakeholders from sectors as varied as transportation and business. These initiatives have also begun reaching out to the defense and security communities, which have a longstanding interest in the health and resilience of military families and communities. Not only is wellbeing neatly complementary to security efforts, but also many security actors have long recognized the importance of wellbeing and have been engaging in wellbeing promotion for years. The U.S. military has sought to support the economic opportunities available to military caregivers, address servicemember mental health, assess "comprehensive soldier fitness," and examine the impact of communication technologies on service members' resilience and wellbeing.[10] The parties involved in these combined efforts could consider how to expand this outreach and strengthen these relationships.

Any efforts to capture and derive value from digital data, whether it is wellbeing- or security-focused, will likely have to grapple with a set of common concerns. As is clear from recent trends, tech ethics and data privacy, along with equity and bias in algorithms, will probably remain among such concerns. Further, while security stakeholders must contend with the private sector's wariness, digital data companies are facing their own reckoning in terms of public trust. Addressing these issues will be important in determining the feasibility and success of future collaborations on tech and security.

Seen from another angle, the major security challenges facing the world may end up resembling wellbeing problems. Automation and a resulting lack of work and opportunity may threaten people's sense of meaning and purpose. Unaddressed mental health issues may precipitate violent incidents. Mass migration can spark regional conflicts. Online hacking and trolling contribute to a breakdown of civic trust and participation and weaken our belief in facts and evidence. Climate change could more frequently spawn severe, deadly weather events.

Ensuring security is the most fundamental responsibility of government. The ability to discharge that responsibility will benefit from continued collaborations with the tech industry and other societal actors to acquire and employ technological capabilities. Security stakeholders already cooperate with a wide range of actors across different countries and with different missions. Going forward, the security and wellbeing communities should consider how the similarities of their missions can inform the best use of digital data to achieve security and wellbeing for all.

[1] Sheera Frenkel, "Microsoft Employees Protest Work With ICE, as Tech Industry Mobilizes Over Immigration," The New York Times, June 19, 2018, <https://www.nytimes.com/2018/06/19/technology/tech-companies-immigration-border.html> (accessed January 17, 2019).

[2] Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees," The New York Times, June 1, 2018, <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html> (accessed January 17, 2019).

[3] See: James Vincent, "Amazon employees protest sale of facial recognition software to police," The Verge, June 22, 2018, <https://www.theverge.com/2018/6/22/17492106/amazon-ice-facial-recognition-internal-letter-protest> (accessed January 17, 2019); Ali Breland, "Amazon employees protest sale of facial recognition tech to law enforcement," The Hill, June 21, 2018, <https://thehill.com/business-a-lobbying/393583-amazon-employees-protest-sale-of-facial-recognition-tech-to-law> (accessed January 17, 2019).

[4] "Homepage," Air Louisville, <https://www.airlouisville.com> (accessed January 17, 2019).

[5] "Making Health a Shared Value," Robert Wood Johnson Foundation, <https://www.rwjf.org/en/cultureofhealth/taking-action/making-health-a-shared-value.html> (accessed January 17, 2019).

[6] See: Amy Maxmen, "Migrants and refugees are good for economies," Nature, June 20, 2018, <https://www.nature.com/articles/d41586-018-05507-0> (accessed January 17, 2019); J. Edward Taylor, Mateusz J. Filipski, Mohamad Alloush, Anubhab Gupta, Ruben Irvin Rojas Valdes, and Ernesto Gonzalez-Estrada, "Economic impact of refugees," Proceedings of the National Academy of Sciences of the United States of America 113 (27) (July 5, 2017): 7449–7453.

[7] Catherine Clifford, "Obama on wealth inequality: 'There's only so much you can eat. There's only so big a house you can have.,'" CNBC, July 18, 2018, <https://www.cnbc.com/2018/07/18/barack-obama-on-wealth-inequality-only-so-much-you-can-eat.html> (accessed January 17, 2019).

[8] "Outcome: Improved Population Health, Well-being, and Equity," Robert Wood Johnson Foundation, <https://www.rwjf.org/en/cultureofhealth/taking-action/outcome-improved-population-health--well-being--and-equity.html> (accessed January 17, 2019); Darren Walker, "Toward a new gospel of wealth," Ford Foundation, October 1, 2015, <https://www.fordfoundation.org/ideas/equals-change-blog/posts/toward-a-new-gospel-of-wealth> (accessed January 17, 2019).

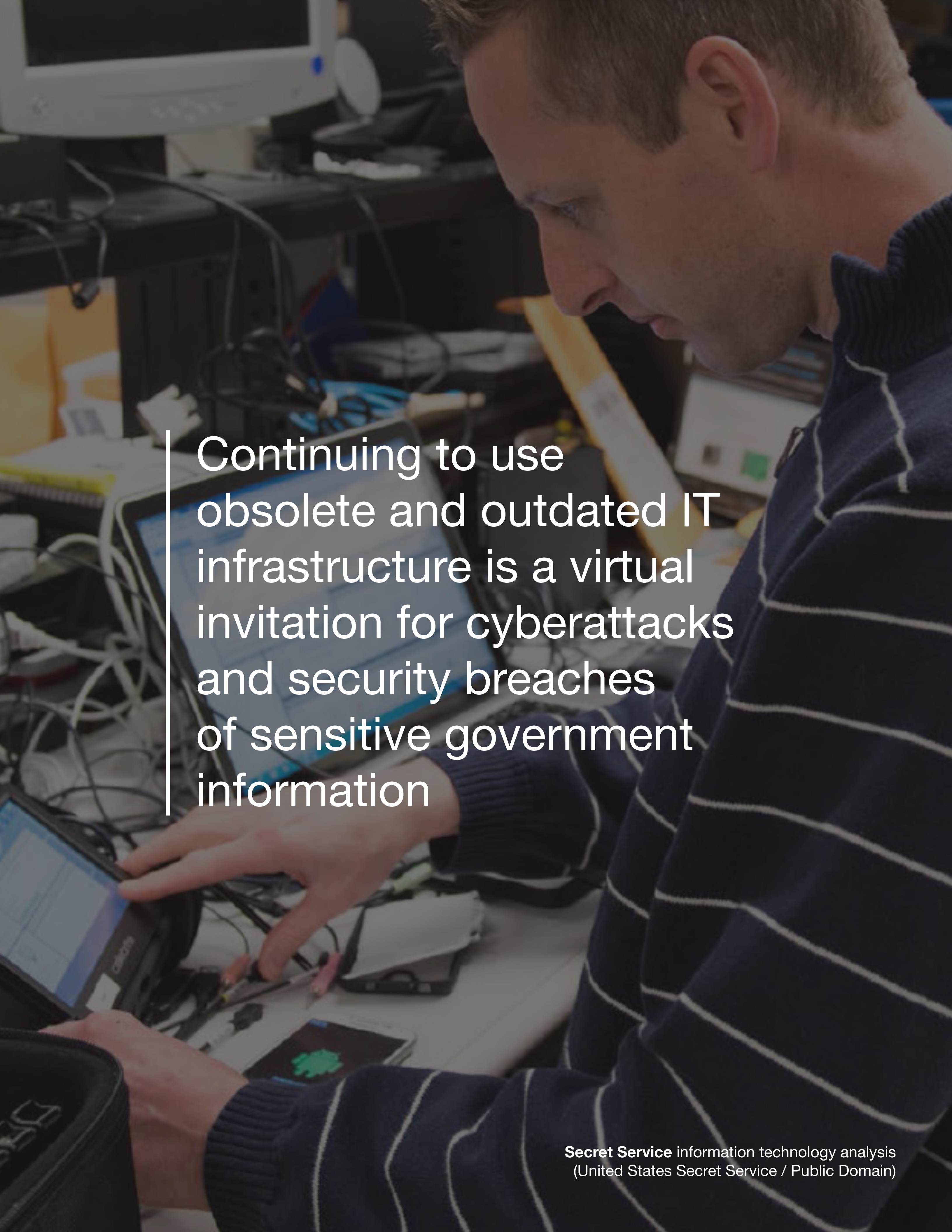
[9] Brenda M. Seaver, "This Is Why Global Income Inequality Is a Real National-Security Threat," The National Interest, September 1, 2015, <https://nationalinterest.org/feature/why-global-income-inequality-real-national-security-threat-13747> (accessed January 17, 2019).

[10] "Comprehensive Soldier & Family Fitness," U.S. Army, <http://csf2.army.mil> (accessed January 17, 2019); Laura L. Miller, Laurie T. Martin, Douglas Yeung, Matthew Trujillo, and Martha J. Timmer, Information and Communication Technologies to Promote Social and Psychological Well-Being in the Air Force: A 2012 Survey of Airmen (Santa Monica: RAND Corporation, 2014), 104.

## Dr. Douglas Yeung

Dr. Douglas Yeung is a behavioral scientist at the RAND Corporation and a member of the Pardee RAND Graduate School faculty. His research examines the societal impact of technology in national security, workforce, and wellbeing policy. His recent work has explored how policymakers can use insight from emerging technologies (e.g., social media, mobile devices) for wellbeing and civic policy-making. Yeung's other research involves online professional communities, and explores workforce attitudes and organizational knowledge-sharing, such as how military recruits discuss and seek career information. He has also conducted workforce diversity research, such as how minorities and women perceive career options. He has published most recently on public trust in the tech industry, and intentional bias in algorithms.

Before coming to RAND, Yeung was a product analyst at Oracle, and also helped to create a mobile application that was a grand prize winner in Google's first Android Developer Challenge. He received a Ph.D. from Rutgers University - Newark, and a B.S. from the Massachusetts Institute of Technology.



Continuing to use obsolete and outdated IT infrastructure is a virtual invitation for cyberattacks and security breaches of sensitive government information

**Secret Service** information technology analysis
(United States Secret Service / Public Domain)

# Obstacles to IT Modernization
## The New National Security Imperative

Richard Beutel & Andrew Caron

### INTRODUCTION

As the December 2018-January 2019 government shutdown pressed forward into unexplored territory, no one asked what impact the continuing funding delays might have upon information technology (IT) modernization. This should be a significant concern, as IT modernization is now widely recognized as a national security imperative. The cumbersome and lengthy acquisition process stifles innovation and allows U.S. adversaries such as China to develop and deploy cutting-edge technologies far faster than the United States is able. The loser is the U.S. military, which is often saddled with obsolete capabilities. The recently released Third Volume of the Section 809 Panel report states this explicitly—we are on a "war footing"—and the government's cumbersome acquisition policies are a primary culprit. The shutdown certainly did not help any of this. The authors can offer no solution regarding how to solve the threat of another shutdown. The issues are no longer substantive—both parties see "the wall" as emblematic to their political base. But we can talk about recent green shoots in addressing the IT acquisition.

Without mincing words or exaggeration, the government has a dismal record of successful IT modernization.[1] The U.S. Government Accountability Office (GAO), a respected government watchdog, has exhaustively documented the government's dependence on outdated legacy IT and the billions of U.S. dollars wasted by agencies in failed modernization attempts.[2] The causes are numerous: a compliance-oriented acquisition workforce, perverse incentives that reward "box checking" rather than end-user outcomes, and an entrenched cultural fear of "doing things differently" caused by an overblown concern about potential bid protests and increased congressional oversight.[3]

Recently, however, a new awareness has arisen across the government that the old ways of IT procurements no longer serve the country. Current acquisition techniques are relics of an age before commercialized internet services even existed; they were not designed to keep pace with the rapid evolution of IT technologies.

Greg Touhill, former Federal Chief Information Security Officer, captured the scope of this challenge. "Touhill's Law" states that, since the average human

**Brig. Gen.** Greg Touhill receives his new rank (Kemberly Groue / Public Domain)

**United States Secretary of Homeland Security** Jeh Johnson attends a DHS Cybersecurity Town Hall meeting (U.S. Department of Homeland Security / Public Domain)

lifespan is seventy-five years, and the average computer's lifespan is three years, for every year a computer exists, it will age the equivalent of twenty-five human years.[4] Given how quickly technology ages, the government cannot continue to use traditional slow-moving acquisition techniques and expect to remain up-to-date in a 21st-century digital world.

The omnipresent and increasing threat of cyberattacks provides further motivation for a more dynamic procurement system, because continuing to use obsolete and outdated IT infrastructure is a virtual invitation for cyberattacks and security breaches of sensitive government information.[5] Recognizing these issues, the Department of Homeland Security's (DHS) Procurement Innovation Lab (PIL), a forward-leaning innovation cell and test-bed for the development of cutting-edge procurement techniques, has identified several key goals that will enable the government to evolve more rapidly, including:

- Lowering entry barriers for innovative, non-traditional contractors;
- Shortening the time-to-award, thereby delivering capabilities to customers faster;
- Encouraging competition by providing interested vendors with an improved understanding of the goals and objectives for each procurement; and
- Increasing the likelihood of successful outcomes by refining evaluation techniques to identify the most qualified contractors.

Ultimately, smart risk-taking, lower proposal development burden, and clear alignment between solicitations and mission objectives help DHS yield better solutions more quickly, improve contract performance, and provide savings to the taxpayer.[6]

The most important recognition, in the authors' view, is the acknowledgement of the time value (or lost opportunity cost) associated with the interminable pace of current acquisition procedures. Metrics such as the "Procurement Acquisition Lead Time" (PALT), the amount of time it takes a contracting officer to award a contract, indicate a growing awareness of the tangible costs of delays in the form of implementation of obsolete systems "out-of-the-box," and the resulting increased cybersecurity risks.[7] [8]

There is also a recognition that, in order to obtain true IT innovation, the government should, indeed must, turn to existing commercial technologies and determine how best to bring them into government.[9]

## THE GROWTH OF COMMERICAL ITEMS: FASA AND BEYOND

The preference toward the federal government using commercial technology has already been the subject of multiple legislative initiatives, starting with the 1994 passage of the Federal Acquisition Streamlining Act (FASA).[10] FASA was designed to streamline the acquisition by introducing simplified acquisition procedures and pushing program offices to buy commercial-off-the-shelf (COTS) items whenever possible by making them much quicker and easier to purchase than traditional acquisition methods.[11] The Act establishes a preference for the government's use and adoption of commercial technologies that provide the best value to the government, rather than focusing solely on the lowest offer.[12] The reason for this transition is simple: the bulk of research and development has migrated from the government to the private sector.[13] The federal government is now hopelessly outclassed in terms of cutting-edge technology development and needs to adapt accordingly.

Both federal chief information officers, as well as their acquisition staff, now realize that meeting the emerging requirements of the Federal IT Acquisition Reform Act (FITARA) as well as Office of Management and Budget (OMB) policies such as Cloud Smart and the recently revised OMB Data Center Consolidation Initiative require extensive reliance upon commercial systems and commercial technologies.[14] To better address these concerns, acquisition professionals have shown, with proper leadership, a remarkable agility in embracing new procurement techniques.[15] Groups such as DHS's PIL have spearheaded training and dissemination of best practices and rapid procurement techniques across multiple program offices.[16] Some of these techniques mimic the approach taken by venture capitalists and others in the private sector.

## TRANSITION FROM FIRM FAR PRACTICES TO FLEXIBLE RAPID ACQUISITION TECHNIQUES

The Federal Acquisition Regulation (FAR) rules were drafted to ensure a uniform standard for acquisition across the entire federal government.[17] It serves as a guidepost for contracting officers (COs) and seeks to ensure that the government receives the best technologies, goods, and services at the fairest price possible.[18] However, the FAR has proven to be ineffective in allowing COs to keep up with the rapid advancement of technology: COs have become consumed by checking boxes, rather than satisfying the needs of the end user.

These regulations have allowed bloated and slow-moving legacy contractors to dominate most IT contracts, utilizing their vast resources to establish offices dedicated to securing government contracts almost perpetually.[19] Meanwhile, nontraditional contractors offering new and innovative technologies are unable to compete due to their lack of experience and inability to meet the bureaucratic requirements. Further, many leading IT companies, such as the ones in Silicon Valley, are unwilling to even attempt to work with government because of its notoriously complex and unfriendly intellectual property (IP) policies attached to traditional procurements.

In response, Congress has been testing the water by implementing rapid acquisition techniques across the

IRD Management Integration Office Chief Amy Kennedy-Reynolds speaks about FITARA (NASA / Public Domain) federal government, including Small Business Innovation Research (SBIR) Phase III, Other Transaction Authority (OTA), and the Commercial Solutions Openings (CSO) Pilot Program. While these programs are a promising starting point, each has unique advantages and disadvantages that should be examined and refined to ensure that the government can effectively keep pace with the technological advancement of the private sector.

The SBIR Phase III program is a glowing example of the U.S. government trying to avoid the grasp of large legacy contractors and looking to smaller start-up businesses for innovation. The goal of this program is to allocate funding to small businesses and non-profit U.S. research institutions so that they can pursue new technological research and develop it in to commercially viable products without fear of sacrificing ownership, IP rights, or future profits.[20] To limit waste of taxpayer dollars, the program utilizes a tranched phase-oriented methodology ensuring that only the most promising, commercially viable products continue to receive resources.[21] Each phase has specific dollar values and time limits with which to comply.[22] Successful awardees move to the next phase, receiving additional funding and the potential for follow-on contracts, while costly and ineffective ideas are scrapped with minimal investment by government.[23]

While the SBIR Phase III technique is an effective way to streamline procurements using the FAR, the first truly rapid acquisition authority that Congress created to bypass the FAR is the OTA.[24] OTAs are flexible agreements that often have minimal standard requirements, other than cost sharing, and are designed to encourage faster research or prototyping with less administrative intervention and overhead costs.[25] Specifically, OTAs allow the government to work directly with the private sector to solve issues in a faster, more effective manner, without having to worry about "checking the boxes" required by the FAR.

OTAs are beginning to gain significant traction with help from programs like DHS's PIL and the Defense Innovation Unit (DIU).[26] However, these awards often require cost-sharing agreements and are only available for specific agencies enumerated by Congress.[27] Despite these drawbacks, OTAs have given smaller innovative tech companies that typically avoid the government, due to FAR-based obstacles, a way to work with the government that is similar to how they conduct business commercially.

While experimenting with OTAs, DIU developed and piloted a new acquisition technique, coined the Commercial Solution Opening.[28] CSOs allow the government to post a general solicitation to fulfill a need without outlining a specific methodology, allowing the private sector to propose unique solutions.[29] The private sector can choose to either develop new technology to meet the need, which would be difficult considering the relatively short PALT, or meet the need with tech that is available commercially with little or even no modification to fulfil the need in the most efficient way possible. These awards are similar to Broad Agency Announcements (BAAs), but rather than being restricted to a general government purpose, CSOs allow for the acquisition of the technology for specific programs.[30] Based on the success of the CSOs, Congress authorized the Department of Defense (DoD) and General Services Administration (GSA) to participate in an official pilot program by the same name.[31]

CSOs are not regulated under the standard rules of the FAR, allowing the contracting officer much more discretion to base the decision on the fulfillment of the needs of the government, rather than a generic selection standard.[32] However, with this discretion comes some significant limitations.[33] Both the GSA and DHS have a hard cap of USD 10 million on any CSO award, while DoD must notify Congress about any award over USD 100 million.[34] Additionally, the authority has only been delegated to the GSA, DHS, and DoD for this iteration of the CSO pilot program.[35]

While none of these techniques are perfect, they have made Congress aware that changes need to be made. With these techniques, contracts are being awarded faster, the government has received more current technology, and contracting failures tend to be caught earlier with less investment by the government. Although these are significant improvements, the government still needs to make modifications to maximize the strength of the rapid acquisition techniques while also eliminating weaknesses indicated by past failures.

## A PROMISING FUTURE FOR INNOVATION: THE IRS PILOT PROGRAM

One potentially disruptive approach is being piloted

**Washington, D.C., USA.** Internal Revenue Service Building (Ken Lund / CC BY-SA 4.0)

by none other than the Internal Revenue Service (IRS). The IRS has one of the most notoriously antiquated legacy infrastructures of any agency across the federal government.[36] In a recent report from June 2018, the GAO noted that the IRS spent USD 2.7 billion on its IT investments in 2016, of which USD 1.9 billion was spent on operation and maintenance of its existing systems.[37] A large portion of these maintenance costs come from the IRS's reliance on legacy programming languages and outdated hardware. These have increased costs from inefficiencies and a lack of qualified IT individuals who can effectively work the outdated systems.[38]

According to the GAO, of the USD 684.2 million in hardware associated with the IRS's Mainframes and Servers Services and Support (MSSS) program, which makes up 73 percent of the IRS's total infrastructure, approximately USD 430.3 million (63 percent) is outdated.[39] Beyond being inefficient, these outdated systems pose increased maintenance costs, upwards of 25 percent more per year, and significant risks to the ability of the IRS to handle its core function: taxes.[40] IRS officials have stated that relying on current MSSS hardware "has the potential to expose IRS to equipment failures that could preclude its systems from supporting the annual tax filing season…."[41] As one can clearly see, it is not a lack of investment or funding by the IRS that is the source of the problem; rather, it is the lack of communication and consultation with IT experts in the private sector.

Facing significant backlash from the GAO and Congress, the IRS reevaluated how it acquired IT services for its deficiencies and created the IRS Pilot Program.[42] This program utilizes a five-phase process involving: communication and discussions with the private sector about the IRS's needs; evaluating potential solutions submitted by the private sector; testing the prototypes on an individual scale; testing an initial deployment at the local scale; and testing a limited/pilot deployment at a regional/national scale.[43] Each phase is tranched with specific time and monetary limits and requires significant merit to progress to the next phase.[44]

Essentially, this process allows ineffective and inefficient ideas to be weeded out at each phase, leaving only the best ideas. From there, the IRS will use follow-on production contracts to select winning solutions to implement. Under the highly respected procurement leadership of programs like DHS's PIL or DIU, this program approach has the possibility of transforming the IRS's legacy IT systems in to a shining example for the rest of the federal government.

## A MODEST LEGISLATIVE PROPOSAL

The U.S. federal government desperately needs to accelerate these emerging techniques. Certainly, one size will not fit all circumstances. However, the pluses and minuses of these techniques outweigh the risks posed by the current status quo. Smart policy development can accelerate this process even further, and legislation

**An electroplater** uses a new coating process developed under the SBIR program (Alex R. Lloyd / Public Domain)

can accelerate this process. While still notional, there are several concepts that need to be adopted across the federal government.

The first concept is the incorporation of OTA and CSO language in all civilian agencies through modification to the public contracting statutes found in Title 41 of the U.S. Code. Through this implementation, the federal government could still utilize the FAR for non-time-sensitive items but have the option to use OTAs and CSOs to capitalize on the innovation of the private sector where necessary. Congress could add controls such as monetary limits, or even penalties, for the abuse of the system, but it is essential that agencies are given more leeway in their decision-making process. The best assurance of success is for Congress to mandate every agency has an acquisition center for excellence following the model of DHS's PIL.

By requiring agencies to adopt these acquisition centers for excellence, Congress would be ensuring that there are always acquisition experts available to contracting officers, regardless of to which agency they belong. These centers would serve as a central hub where contracting officers can receive training, ask questions, learn about best practices and reevaluate what it means to achieve the best results for the government. Additionally, by having all these hubs communicate with one central "acquisition excellence leader," information could easily be disseminated, whether it be about a new acquisition method, shining examples, or practices to avoid.

Finally, phase-based acquisition should be incorporated into all acquisitions. SBIR Phase III has shown to be an effective way to progress a solution from an idea through to production and fielding with minimal risk or investment by the government but maximum innovation and speed of implementation of the solution. By adopting a phase system where the government allows business to fail fast and fail cheaply, it effectively limits its liability while also serving as a chance for the government to gain insight in to what types of solutions to avoid in the future. Additionally, phase-based acquisitions couple well with bounties and other prize-based awards, which have shown to be effective at encouraging innovative solutions from smaller universities and research institutions that often lack the ability to contract with the government. By utilizing prizes in early phases of acquisition, the government can receive solutions for very little upfront cost and utilize the solutions in future phases or solicitations.

## CONCLUSION

The United States' IT sector is one of the most advanced and prosperous in the world. Meanwhile, the government's most critical IT infrastructures, such as those controlled by the Internal Revenue Service, are severely outdated legacy systems that have a high risk of failing or succumbing to cyberattacks that jeopardize national security. The government cannot hope to consolidate, protect, and transform its aging base of legacy IT without doing something dramatically different in terms of its acquisition procedures. If the hope and promise of a 21st-century digital government is to be fulfilled, we need to enthusiastically embrace risk-taking and the "need for speed" in our core procurement practices. Only in this fashion can government evolve into the 21st century.

[1] *See Information Technology: Implementation of Recommendations is Needed to Strengthen Acquisitions, Operations, and Cybersecurity*, Government Accountability Office report GAO-19-275T, December 12, 2018; *Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks in Tax Processing*, Government Accountability Office report GOA-18-298, June 28, 2018; and *Information Technology: Agencies Need Better Information on the Use of Noncompetitive and Bridge Contracts*, U.S. Government Accountability Office report GOA-19-63, December 11, 2018.
[2] Ibid.
[3] *See* Department of Homeland Security, Office of the Chief Procurement Officer, *Procurement Innovation Lab: Annual Report Fiscal Year 2017* (Washington, DC: Department of Homeland Security, 2018), 4.
[4] Amanda Ziadeh, "Former First Federal CISO Explains the State of Cyber in Government, Says We're Still 9 Years Behind Schedule," Government CIO Media and Research, July 5, 2018, <https://governmentciomedia.com/inside-white-houses-cybersecurity-risk-report>.
[5] *See Information Technology: Implementation of Recommendations is Needed to Strengthen Acquisitions, Operations, and Cybersecurity.*
[6] Department of Homeland Security, Office of the Chief Procurement Officer, 4.
[7] *See* David Berteau, "DoD Can Reduce Time to Contract," *Federal Times*, March 30, 2018, <https://www.federaltimes.com/acquisition/2018/03/23/dod-can-reduce-time-to-contract>.
[8] Ibid.
[9] *See* Erin L. Toomey, "Government Contracts: Reduced Risk Through Commercial Item Contracting," *Practical Law* (2015), < https://www.foley.com/files/Publication/75068fb6-1936-47e3-a9b5-6c4b756558a1/Presentation/PublicationAttachment/2415485f-12ab-426c-99c5-723e63d46c96/Government-Contracts-Reduced-Risk-Through-Commercial-Item-Contracting.pdf>; and *Federal Acquisition Streamlining Act of 1994*, 103rd Cong., 2nd sess., S. 1587 (January 25, 1994).
[10] Ibid.
[11] Ibid.
[12] *See* Federal Acquisition Streamlining Act of 1994.
[13] *See* Toomey.
[14] *Report to the President on Federal IT Modernization*, CIO Council report, 2017, https://itmodernization.cio.gov/assets/report/Report%20to%20the%20President%20on%20IT%20Modernization%20-%20Final.pdf.
[15] *See* Department of Homeland Security, Office of the Chief Procurement Officer, 13.
[16] Ibid., 12-13.
[17] *See* FAR 1.101.
[18] Ibid., 1.102-1.
[19] *See* Mark Micheli, "These are the Top 10 Government Contractors," *Bloomberg Government*, June 15, 2016, <https://about.bgov.com/blog/these-are-the-top-10-government-contractors>; and Neel Mehta, "Bloomberg Government Unveils its 2017 List of Top Federal Contractors," *ExecutiveBiz*, August 24, 2017, <https://blog.executivebiz.com/2017/08/bloomberg-government-unveils-list-of-top-federal-contractors-in-fiscal-2016>.
[20] "About SBIR," Small Business Innovation Research, <https://www.sbir.gov/about/about-sbir> (accessed January 8, 2019).
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] "Acquisition in the Digital Age: Other Transaction Authority (OTA)," Mitre, <https://aida.mitre.org/ota> (accessed January 8, 2019).
[25] Ibid..
[26] Ibid.
[27] Ibid.
[28] *DIUx Commercial Solutions Opening: How-to Guide*, Defense Innovation Unit Experimential report, November 30, 2016, https://www.diux.mil/download/datasets/740/CSOhowtoguide.pdf.
[29] Ibid., 10-16.
[30] *See* "Contracts & Legal: Commercial Solutions Opening," AcqNotes, <http://acqnotes.com/acqnote/careerfields/commercial-solutions-opening> (accessed January 8, 2019).
[31] *See* National Defense Authorization Act for 2017, Pub. L. No. 114-328, § 879, 130 Stat. 2312-13 (2016); National Defense Authorization Act for 2017, Pub. L. No. 114-328, § 880, 130 Stat. 2313-14 (2016)
[32] *See* "Contracts & Legal: Commercial Solutions Opening."
[33] *See* National Defense Authorization Act for 2017, Pub. L. No. 114-328, § 879, 130 Stat. 2312-13 (2016); National Defense Authorization Act for 2017, Pub. L. No. 114-328, § 880, 130 Stat. 2313-14 (2016)
[34] Ibid.
[35] Ibid.
[36] *See Information Technology: IRS Needs to Take Additional Actions to Address Significant Risks in Tax Processing.*
[37] Ibid., 5.
[38] Ibid., 19-22.
[39] Ibid., 19.
[40] Ibid., 20.
[41] Ibid.
[42] "IRS Pilot Program: Solicitation Number: IRS_Pilot_0000," Federal Business Opportunities, November 29, 2018, https://www.fbo.gov/index?s=opportunity&mode=form&id=a6da25883bfbdc9fc21e8d248ddda750&tab=core&_cview=1.
[43] Ibid.
[44] Ibid.

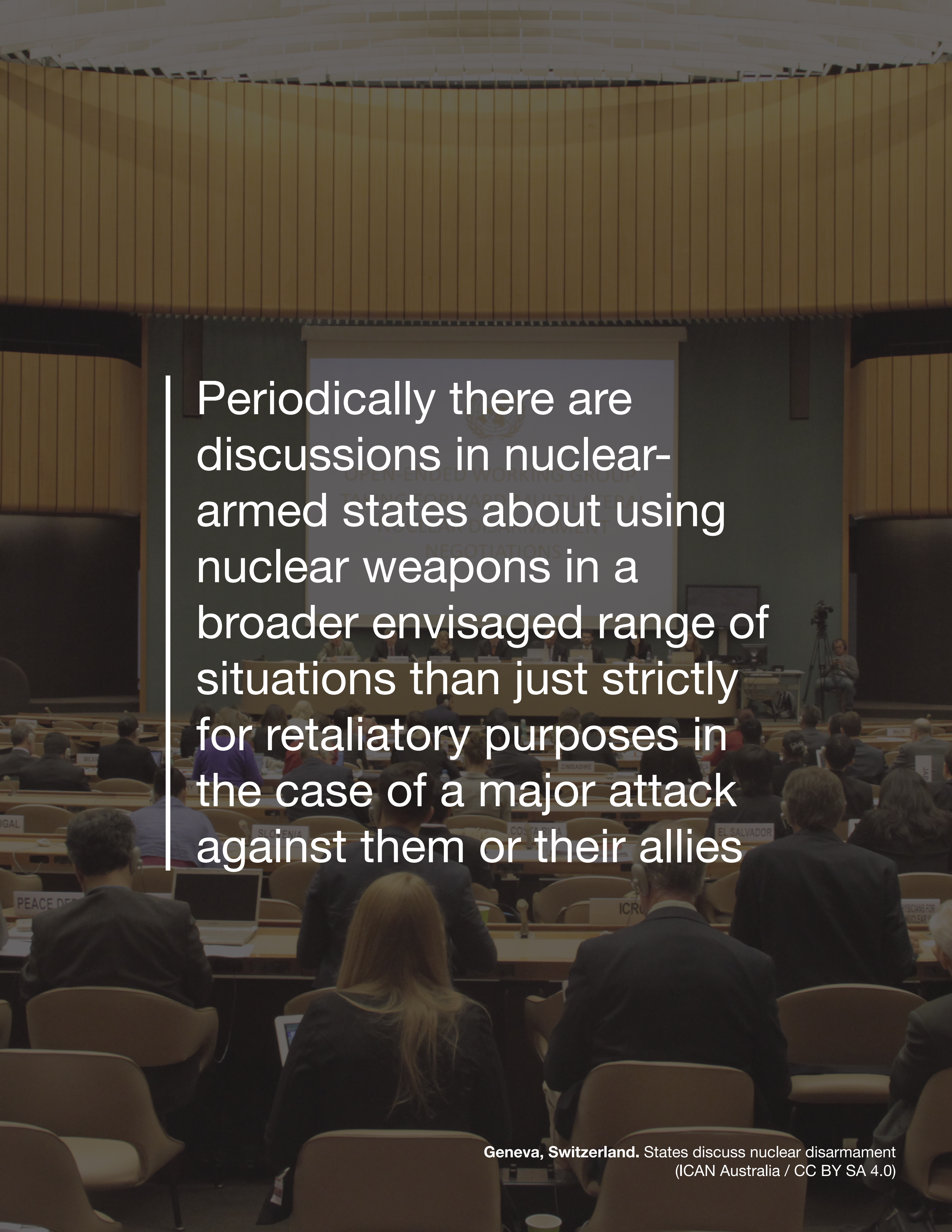
## Richard Beutel

Richard Beutel leads Cyrrus Analytics. Beutel is the former lead acquisition and procurement policy counsel for former Chairman Darrell Issa of the House Oversight and Government Reform Committee. In that capacity, Beutel wrote and managed the Federal IT Acquisition Reform Act, or FITARA, which was signed into law as part of the FY2015 National Defense Authorization Act.

Beutel has bicameral Congressional experience, previously serving as lead oversight and acquisition policy counsel for Senator Susan Collins, the formerly ranking member of the Senate Homeland Security and Government Affairs Committee.

## Andrew Caron

Andrew Caron is a 3L at George Washington University Law School. He received his B.S. and B.A. degrees in International Business and Political Science from Saint Joseph's College of Maine. He contributed to the Section 809 Panel's second and third volume reports and serves as Article Editor for GW's Public Contract Law Journal.



> Periodically there are discussions in nuclear-armed states about using nuclear weapons in a broader envisaged range of situations than just strictly for retaliatory purposes in the case of a major attack against them or their allies

**Geneva, Switzerland.** States discuss nuclear disarmament
(ICAN Australia / CC BY SA 4.0)

# Nuclear Weapons with 21$^{st}$ Century Technology

## A Conversation with John Borrie

Interviewed by FSR Staff

**Fletcher Security Review:** To begin, could you describe your current role at the UN?

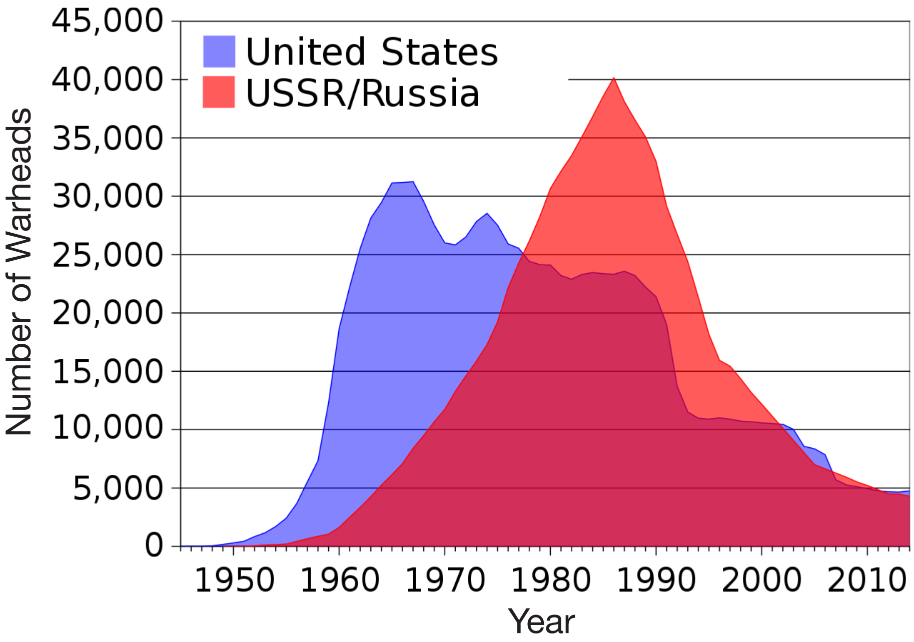
**John Borrie:** Sure. Well, I'm the chief of research at the UN Institute for Disarmament Research or UNIDIR. We're a voluntarily funded autonomous research institute within the UN family. We carry out independent research on all aspects of disarmament and arms control. My job here is to advise the director, oversee the development of the research program, carry out quality assurance on our research as well as to do my own research.

**FSR:** What is your research currently focusing on?

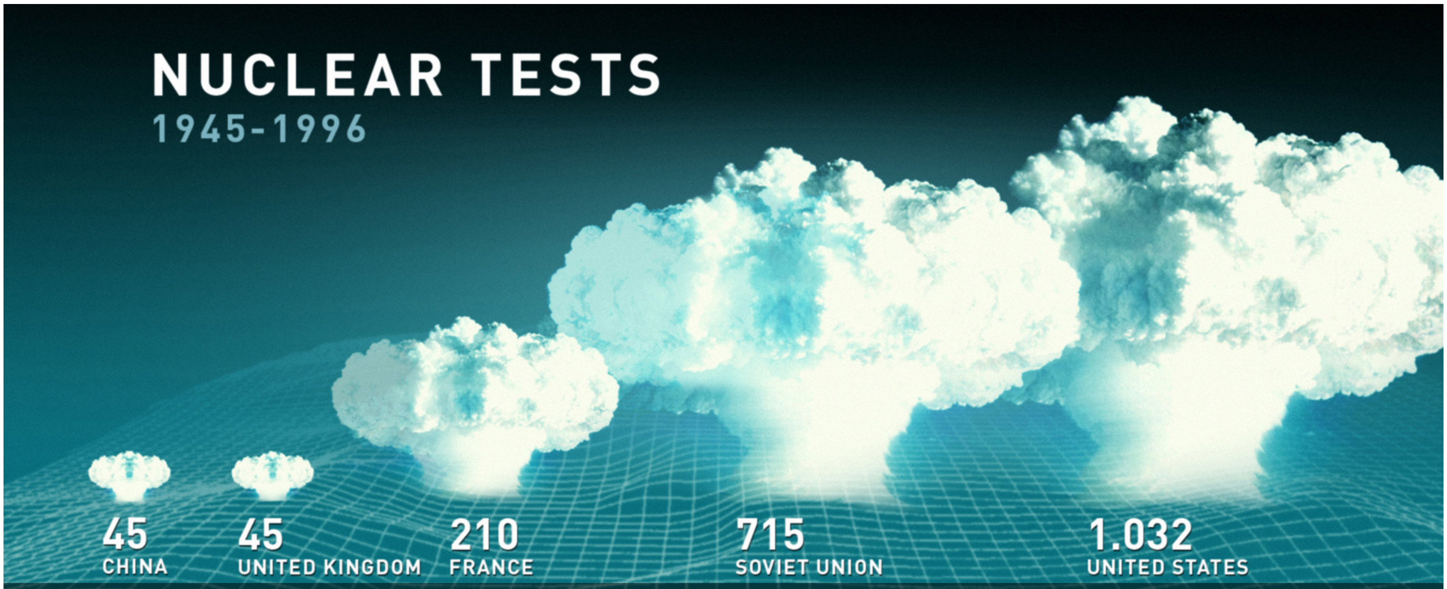
**JB:** Well, I focus on different things at different times. My major interests at the moment include issues around nuclear disarmament and deterrence policies, and technology such as a hypersonic missiles, which could have an impact on nuclear stability. I've been doing some work in the context of oversight and accountability mechanisms for the use of armed un-crewed aerial vehicles (UAVs)—drones—including their implications for stability. I've also been involved in a project here on gender and disarmament. Lastly, I also have an interest in research that is aimed at informing efforts to try to enhance civilian protection from the use of explosive weapons in populated areas. I do all sorts of stuff, but nuclear is sort of my "bread and butter."

**FSR:** So for countries like the United States or Russia, what conditions do you think would need to be created for them to make steps in the direction of a nuclear-free world?

**JB:** Well, it depends. I think that there are some, such as Professor Nick Ritchie, who argue that nuclear weapons need to be devalued in their policies, practices and doctrines. Nuclear weapons are seen as politically very important by quite a few states at the moment—not just states that have them, but some other states who want them or might like to have them in the future. Nuclear weapons are associated with status. And periodically there are discussions in nuclear-armed states (such as Russia and the United States) about using nuclear weapons in a broader envisaged range of situations than just strictly for retaliatory purposes in the case of a major attack against them or their allies.



**Source data from:** Robert S. Norris and Hans M. Kristensen, "Global nuclear stockpiles, 1945-2006," *Bulletin of the Atomic Scientists* 62, no. 4 (July/August 2006), 64 - 66



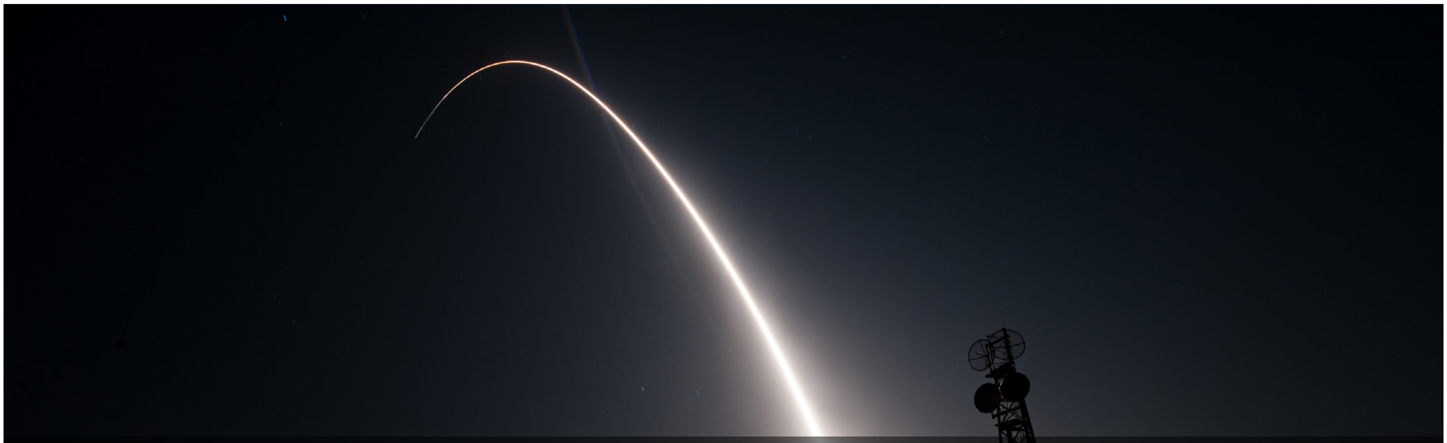
**Breakdown** of nuclear tests 1945-1996 (CTBTO / CC BY 4.0)

Personally, I think that if we are going to move away from nuclear weapons, then it will demand a change of perception and minds of policymakers about the utility of these weapons, as well as other elements such as strengthening of the norm against their use. That could come about in a number of different ways, but it's going not going to be easy. One of the issues with nuclear weapons is that this technology is more than 70 years old, and some of the ways policymakers have of thinking about those weapons and nuclear deterrence are almost that old, and are very deeply embedded. During the Cold War we essentially had a bipolar confrontation between the US and the Soviet Union and their respective allies, and now we have a much more complicated world in which we have a number of technologies that call into question the continued applicability of nuclear weapons for deterrence purposes because of the ambiguity they create in crisis situations. For example, cyber offensive capabilities, which are difficult to attribute to any particular actor, may not necessarily physically damage to a society's infrastructure or kill anyone. But offensive cyberoperations might be very damaging—even crippling—in terms of theft of money or intellectual secrets or personal data about people. It's challenging to see how nuclear weapons can be used coherently to deter that.

At UNIDIR, we're also looking at implications of other technologies which are becoming entangled with nuclear weapons and nuclear doctrines. For example, space-based infrastructure is pretty crucial to some modern nuclear command and control systems. Attacks on or threats to that infrastructure might be taken by certain countries like the US, China and Russia as demanding a response with nuclear weapons before they lose the capability to do so. Then there are also new advanced conventional missile capabilities that are specifically designed to overcome missile defenses to destroy high value targets, which might include nuclear command and control. All of these create ambiguity in terms of nuclear doctrines and practices. These are headaches for nuclear policy makers, not to mention the fact that we have nine nuclear states, not five, and crisis communication between these states…It's not especially good.

**FSR:** In terms of new technologies, which do you see or have you already seen becoming entangled with nuclear technologies? Is AI going to be a part of the nuclear conversation?

**JB:** A lot of current discussion about AI is largely speculation. I mean, I've just mentioned space. We can already see it because we've got at least three states that have already tested anti-satellite capabilities. The United States, China, and Russia all have tested surface-based capabilities that could knock out satellites, some of which are important for nuclear command and control. So, this entangles it further. And if countries start militarizing space to an even greater extent than is already the case, for example, by placing weapons there, then



**Vandenberg Air Force Base, USA.** An unarmed Minuteman III ICBM launch test (SrA. Ian Dudley / Public Domain)

that will create further entanglement with new missile capabilities as I just mentioned. Then there are missile defenses themselves, which incrementally are improving in some ways. This can create fears, for example, in China or Russia, that the US won't be vulnerable anymore to nuclear retaliation, at which point nuclear deterrence breaks down for them. Then you've got cyber. We've already seen evidence presented by people like David Sanger, the New York Times journalist, and others, of cyber hacking of very important systems, for example, in North Korea by the US as well as North Korean hacking of economic targets like Sony Pictures. Earlier we saw Stuxnet impacting the Iranian centrifuges. It's not inconceivable that nuclear command and control systems might be vulnerable to cyber offensive operations. All of these things can introduce ambiguity about nuclear command and control chains. They can potentially create "use it or lose it" situations.

And then you've got so-called autonomous weapons or increasing autonomy in weapon systems as we tend to think about it in UNIDIR. You've got autonomy-in-motion systems like loitering munitions or in increasingly autonomous drones. And then on the other hand, you've got autonomy-at-rest systems. These latter capabilities might come to play a role in nuclear command and control systems because of the speed of warfare and the huge amount of sensory information coming in. It means nuclear decision makers may come to rely on "machine learning" or other technologies described as "AI" to help triage and sort information in order for them to make timely decisions. Now the issue with that is you can't necessarily see how these systems are operating in real time and what assumptions they were operating on, so that can potentially create some issues since its difficult, among other problems, to instill contextual understanding into algorithm-based systems.

A RAND study from earlier this year said that some of these AI techniques will make it easier, potentially, to find mobile ICBM launches. That can create "use it or lose it" situations. If you're in China and you think that the United States knows where all of your nuclear missiles are and could attack them, then you might be tempted to use them before they're destroyed. Conversely, if you're on the other side you might feel very tempted in a crisis situation to strike preemptively to take those launchers out of commission. All of these prospects would create ambiguity, and ambiguity, when we're dealing with crisis escalation, is bad. But right now, we're right at the outset of the "AI age" and it's hard to predict how these technologies and related military capabilities are going to evolve.

## John Borrie

John Borrie is the research coordinate and program lead at the United Nations Institute for Disarmament Research. He's currently working on continuing and expanding dialogues about disarmament and the impact of nuclear weapons on humanitarian affairs. He previously worked on weapons control for both the International Committee of the Red Cross and as a New Zealand diplomat. Borrie holds a doctorate in philosophy from the University of Bradford.

> As electrification has come to drive all commerce and government, making it a key element of the country's national security, what is the best way to protect the grid from terrorist, weather, or cyber-related threats or attacks?

**Satellite image** of the continental United States at night
(NASA / Public Domain)

# Resilient Power

## A New Model for Grid Security

Lewis Milford & Samantha Donalds

In the last few years, Washington has been preoccupied with a debate about the security of the nation's electric grid. The debate is as old as the grid itself: as electrification has come to drive all commerce and government, making it a key element of the country's national security, what is the best way to protect the grid from terrorist, weather, or cyber-related threats or attacks?

As with most things of a political nature, where you stand depends on where you sit.

Proponents of coal, oil, and nuclear make the argument that traditional large-scale power plants are not only vital to grid stability, but also that this centralized generation model is the only economically or technologically feasible option.[1] It's an old argument wrapped in new national security rhetoric, and it's increasingly straining against the facts. More and more analysis and real-life examples show that distributed renewable energy, combined with energy storage technologies, can provide reliable power more affordably and reliably than the centralized generation alternatives.

The argument in favor of large-scale power plants is also based on incorrect assumptions about the true nature of grid stability. According to a recent study:

The vast majority of outages across the power system are caused by weather events rather than generation-level failures (including fuel supply failures). Furthermore, most outages caused by natural events harm electric T&D transmission and distribution assets in common ways, leading to the conclusion that the most practical way to improve resilience and reliability is to address T&D and grid operations rather than generation and fuel issues.[2]

In other words, the real threats – and solutions – to grid security occur not at the central generation level but at the local distribution level.

The U.S. electrical distribution system is a massive, outdated, and extremely fragile web of poles and wires. It is vulnerable not only to weather, but also to car crashes and squirrels. One small incident can cause a large and prolonged blackout. In the much less likely scenario of a terrorist attack on the electrical grid, the target would not be the distribution system but rather at the central generation or substation level, for maximum impact and ease of targeting.[3] In both scenarios, whether an outage is accidental or intentional, the centralized nature of our grid is a serious liability.

The best solution to the national security problem posed by power outages is the new field of distributed "resilient power.

### WHAT IS RESILIENT POWER?

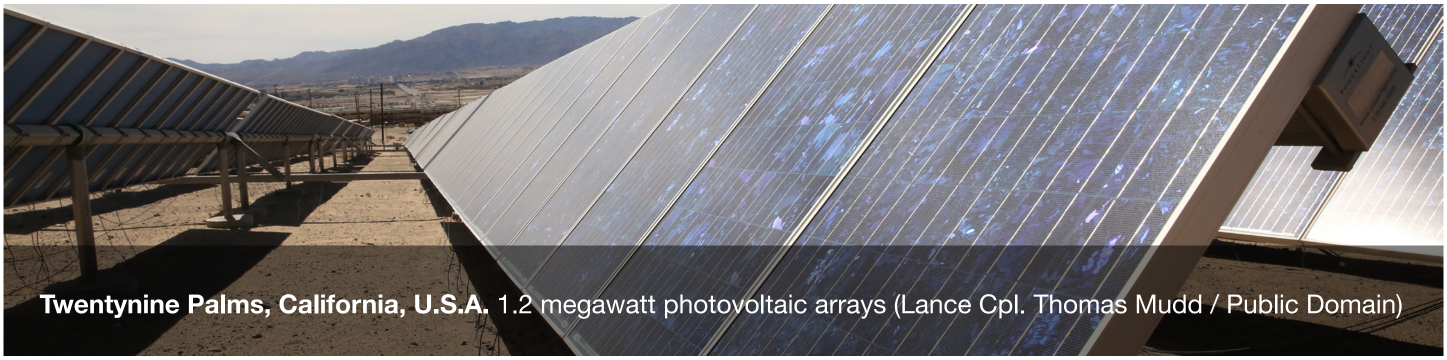
"Resilient power" is the ability to provide continuous, reliable power to critical facilities and services if the main grid goes down. In order to be truly resilient, the energy generation should be clean and affordable.

Resilient power systems include the following elements:

- Distributed generation. Smaller-scale clean energy resources located at, or near, the sites where the power will be used. Reduced transmission distance is both more affordable and more secure. Energy sources can include renewables like solar or wind or combined heat and power (CHP) systems.[4]

- Energy storage. Energy storage is often called the "holy grail" of the clean energy revolution for a good reason: it allows us to store clean solar and wind power for use when the sun isn't shining, and the wind isn't blowing. This is both an environmental and economic win.

- Smart grid technology. This includes the ability for building energy systems to act as a "microgrid" by islanding and disconnecting from the main grid, the ability to use energy storage for grid services, as well



**Twentynine Palms, California, U.S.A.** 1.2 megawatt photovoltaic arrays (Lance Cpl. Thomas Mudd / Public Domain)

as the ability to protect from cyberattacks.

## HOW RESILIENT POWER SYSTEMS WORK

One of the most economically resilient power technology combinations is a solar photovoltaic system (PV), combined with energy storage (solar + storage).

When the main grid is functioning normally, the solar panels will generate power during daylight hours. The battery storage system will save excess generation for use during a power outage and be deployed for electric bills savings and monetizable grid services at strategic times.[5]

During the event of an outage, the solar + storage system will disconnect from the grid, allowing it to safely supply power to critical building loads, such as heating, common area lighting, or refrigeration. These "microgrid" systems can also be completely independent from the main grid, allowing the energy systems to provide 100 percent of a building's power needs at all times.

In the town of Sterling, Massachusetts, a solar + storage microgrid can power the town's police station and emergency first responder facility for up to 12 days in the event of a grid outage. Besides the benefits to community safety, the Sterling microgrid also has excellent economics, saving ratepayers USD 400,000 per year.[6]

Energy storage systems paired with other renewable technologies function similarly to solar + storage systems and provide a similar range of benefits. For example, the remote island community of Kodiak, Alaska relies on a wind+ hydro+ storage microgrid for clean, resilient, and affordable power.[7]

## HOW RESILIENT POWER ENHANCES SECURITY AND SAVINGS

Resilient power technologies could benefit almost any facility type, from Walmart[8] to the U.S. military, but they are also well suited for facilities that support low-income and vulnerable populations (affordable housing, nursing homes), medical facilities (clinics, hospitals), and other critical community resources (fire stations, emergency shelters, wastewater treatment plants) where prolonged power outages could be catastrophic to local communities.[9]

Resilient power technologies make economic sense for many commercial customers, but not all – though the economics are greatly improved when the avoided costs of power outages are considered.[10] These costs can be substantial; power outages from Hurricane Sandy cost an estimated USD 27-52 billion in economic losses, including lost wages, spoiled inventory, and damage to the grid.[11]

## HOW STATE AND LOCAL POLICY IS HELPING THE TRANSITION TO RESILIENT POWER

Following Hurricane Sandy's historic destruction and outages, states and municipalities began to develop programs to encourage the development of resilient power projects in their communities. Examples of state programs include the Massachusetts Community Clean Energy Resiliency Initiative,[12] Maryland's Community Resiliency Hub Grant Program,[13] and Puerto Rico's Disaster Recovery Action Plan.[14] Successful programs share many of the following elements: recognition of the importance of providing critical services in an emergency, prioritization of low income and otherwise vulnerable communities, provision of adequate funding and technical assistance, and support for a variety of use cases.

Policymakers take note: as disasters like Sandy and Maria become the new normal, the economic and humanitarian case for resilient power will only become more potent. To lessen the devastation and economic impacts from future power outages, we need a new definition of national strategy to include a resilient, distributed model of grid security.

[1] “The resiliency of the nation's electric grid is threatened by the premature retirements of power plants that can withstand major fuel supply disruptions caused by natural or man-made disasters and, in those critical times, continue to provide electric energy, capacity, and essential grid reliability services. These fuel-secure resources are indispensable for the reliability and resiliency of our electric grid - and therefore indispensable for our economic and national security. It is time for the Commission to issue rules to protect the American people from energy outages expected to result from the loss of this fuel-secure generation capacity.” From “Notice of Proposed Rulemaking for the Grid Resiliency Pricing Rule,” *Microgrid Knowledge,* September 2017, pages 2-3. [2] Alison Silverstein et al., “A Customer-focused Framework for Electric System Resilience,” May 2018, page 13, <https://gridprogress.files.wordpress.com/2018/05/customer-focused-resilience-final-050118.pdf>.

[3] See: Thomas Griffith, "Strategic Attack of National Electrical Systems," *Air University Press*, 1994, <https://apps.dtic.mil/dtic/tr/fulltext/u2/a425504.pd>; For a recent example, see the 2014 attack on a substation in California: Rebecca Smith, “Assault on California Power Station Raises Alarm on Potential for Terrorism,” *Wall Street Journal*, Feb. 5, 2014, <https://www.wsj.com/articles/assault-on-california-power-station-raises-alarm-on-potential-for-terrorism-1391570879>.

[4] Combined heat and power (CHP), also known as cogeneration, is an on-site power generation unit which produces and uses both electricity and heat. CHP systems are considered to be energy efficient because they make use of heat that would otherwise be wasted, and they can also be considered "clean" if powered by biomass rather than fossil fuels. CHP systems are commonly found on college campuses, hospitals, manufacturing facilities, and other large institutions. Learn more at https://www.epa.gov/chp/what-chp.

[5] Lars Lisell, “When Does Energy Storage Make Sense? It Depends,” *National Renewable Energy Laboratory*, Feb. 28, 2018, <https://www.nrel.gov/state-local-tribal/blog/posts/when-does-energy-storage-make-sense-it-depends.html>. [6] “Sterling Municipal Light Department Energy Storage System,” *Clean Energy Group*, 2018 <https://www.cleanegroup.org/ceg-projects/resilient-power-project/featured-installations/sterling-energy-storage/>.

[7] Rachel Waldholz, “What can Kodiak teach the world about renewable energy? A lot,” Alaska’s Energy Desk, KTOO Public Media, Sept. 15, 2017, <https://www.ktoo.org/2017/09/15/can-kodiak-teach-world-renewable-energy-lot/>.

[8] Seth Mullendore, “Walmart + SolarCity = Solar+Storage,” *Clean Energy Group*, November 2014, <https://www.cleanegroup.org/walmart-solarcity-solar-storage/>. [9] “Featured Resilient Power Installations,” *Clean Energy Group,* <https://www.cleanegroup.org/ceg-projects/resilient-power-project/featured-installations/>.

[10] “Valuing the Resilience Provided by Solar and Battery Energy Storage Systems,” *National Renewable Energy Laboratory and Clean Energy Group*, 2018, <https://www.cleanegroup.org/ceg-resources/resource/valuing-resilience-solar-battery-energy-storage/>.

[11] “Distributed Solar PV for Electricity System Resiliency,” *National Renewable Energy Laboratory,* 2014, <https://www.nrel.gov/docs/fy15osti/62631.pdf>. [12] Todd Olinsky-Paul, “Massachusetts Gets Serious About Resilient Power,” *Clean Energy Group*, July 2018, <https://www.cleanegroup.org/massachusetts-gets-serious-about-resilient-power/>. [13] Maryland Energy Administration - Resiliency Hub, <https://energy.maryland.gov/Pages/Resiliency-Hub.aspx>.

[14] “As Hurricane Michael damages the Southeast, Puerto Rico provides lessons on resilient power,” Lew Milford, Clean Energy Group, October 23, 2018 <https://www.cleanegroup.org/as-hurricane-michael-damages-the-southeast-puerto-rico-provides-lessons-on-resilient-power/>.

## Lewis Milford

Lewis Milford is president and founder of Clean Energy Group (CEG) and Clean Energy States Alliance (CESA), two national nonprofit organizations that work with state, federal, and international organizations to promote clean energy technology, policy, finance, and innovation. He is also a nonresident senior fellow at the Brookings Institution. He works with many public agencies and private investors in the United States and Europe that finance clean energy. He is frequently asked to appear as an expert panelist at energy conferences throughout the United States and Europe. His articles on clean energy have appeared in many print and online publications including The New York Times, The Boston Globe, The National Journal, The Huffington Post, and Renewable Energy World. Before founding these two organizations, he was Vice President of Conservation Law Foundation, New England’s leading environmental organization. Prior to that, he was a government prosecutor on the Love Canal hazardous waste case in New York and previously directed the Public Interest Law Clinic at American University Law School where he represented veterans on a range of legal issues, including gaining compensation for their harmful exposure to Agent Orange and nuclear radiation. He has a J.D. from Georgetown University Law Center.

## Samantha Donalds

Samantha Donalds serves as Communications Coordinator for Clean Energy Group and Clean Energy States Alliance (CESA). Her responsibilities include coordinating the production of webinars and e-newsletters for both organizations; managing content for CEG and CESA’s social media accounts; developing press releases and other media outreach materials; and assisting with publications and events. Samantha produces two of CESA’s monthly newsletters, The CESA Brief and the CESA Members Newsletter. She also serves as webmaster for CEG and CESA websites. Samantha previously worked as an administrator at Fairewinds Energy Education, a nuclear safety advocacy non-profit in Burlington, Vermont. She has also worked as a research assistant in the environmental studies department at Brown University, where she researched fisheries projects in West Africa and compiled historic climate and fisheries data from southern New England. Samantha graduated cum laude from Mount Holyoke College with a B.A. in Environmental Studies and a minor in French. Samantha is currently pursuing a Masters in Energy Regulation and Law at Vermont Law School.

> A low-grade separatist insurgency continues to fester in Baluchistan, and separatists will continue to target energy infrastructure when they sense good opportunities

**Flag** of the Balochistan Liberation Army
(Vif12vf / CC BY-SA 4.0)

# Insufficient Energy Technology in Pakistan

## A Conversation with Michael Kugelman

Interviewed by Arthur Sanders Montandon

**Fletcher Security Review**: Pakistan's energy infrastructure is notoriously problematic. In your 2015 essay "Easing an Energy Crisis That Won't End," you wrote that China's recent investment of USD 35 billion in energy projects in Pakistan will not be enough to solve the country's chronic issues such as recurring power outages, inefficient infrastructure-induced debt, and wasteful transmission and distribution mechanisms that waste up to 20 percent of the energy produced in the country. You pointed out that the root cause of this is not only insufficient energy supply, but bad governance. Non-state armed groups, such as the Pakistani Taliban in April 2013 and Balochi insurgents in January 2015, have targeted Pakistan's energy installations to further deteriorate the government's ability to provide basic goods to its population.

Since the essay was published, what has been the Pakistani government's energy policy and how do you evaluate it? What are the effects of Pakistan's energy crisis on the country's stability and security environment?

**Michael Kugelman**: The Pakistani government, which has been on the defensive for several years due to anti-government protests and corruption allegations, deserves some credit here. The ruling Pakistan Muslim League Party-Nawaz (PML-N) was swept into power in 2013 with a mandate to fix an energy crisis that had become so acute that you had power outages of up to 15 hours a day in some areas in the summer months. The crisis had major negative impacts — such as electricity-less factories having to shut down and lay off their employees — on the economy. Today, the energy crisis is still there, but it has eased at least modestly. The daily outages are not as long, and perhaps most importantly the debt within the energy sector — which had ballooned to several billion dollars at one point several years ago — has been reduced after the government acquired money from commercial banks to finance the debt.

The verdict is split, however, on why Pakistan has arrived at this better point. The government and its supporters will point to effective policy — such as adding

**Mangla Dam, Pakistan.** United States Ambassador pledges new support to alleviate the energy crisis (U.S. Embassy Pakistan / CC BY-ND 4.0) more electricity to the grid through a series of newly inaugurated power plants. Detractors, however, will suggest that external factors — like cheaper global oil prices and robust flows of remittances into Pakistan— have been more responsible for helping ease the crisis. Ultimately, the truth may be somewhere in between. The bottom line, however, is that the root causes of the energy crisis remain entrenched. These include poorly functioning infrastructure that lead to transmission and distribution losses in excess of 20 percent, distorted pricing regimes that result in people not paying their energy bills and not getting penalized for it, and above all institutional dysfunction that involves too many ineffective government agencies being saddled with energy-related responsibilities. It's just a matter of time before the energy crisis flares up in a big way once again.

In a volatile country like Pakistan, energy insecurity can have troubling implications for stability. On small-scale levels, this can include violent protests in cities when the power goes out on very hot days. On broader levels, militants can try to exploit energy vulnerabilities. As you note, two prime sources of anti-state violence — Islamist militants and separatist insurgents — have frequently attacked power grids, knowing that taking out a single grid station can plunge large parts of the country into darkness. The good news is we haven't seen these types of attacks as frequently since 2015. A big reason for that is the effectiveness of a Pakistani military counterterrorism offensive against anti-state terror groups, particularly the Pakistani Taliban, which was launched in 2014.

Still, a low-grade separatist insurgency continues to fester in Baluchistan, and separatists will continue to target energy infrastructure when they sense good opportunities. The Baluchistan insurgency is in itself a strong case study of the tight links between energy insecurity and instability. The insurgency is fueled, in great part, by what locals perceive to be the inequitable exploitation of Baluchistan's abundant natural gas riches. The Baluch accuse the state, often with the connivance of private companies, of extracting natural gas without ensuring that sufficient amounts remain for local use. It's a very similar dynamic to the Naxalite insurgency in India, where communities in eastern India — mainly Chhattisgarh state — accuse the government of preying on coal resources while ignoring the needs of local residents.

A similar dynamic could well play out in Pakistan in the coming years. In the southern province of Sindh, 175 billion tons of coal reserves lie untouched. For years, Pakistan has tried to figure out how to extract them, but it's lacked the right technology. Now, with China investing deeply in Pakistan as part of its China-Pa-

**Hindu Sena members** hold a Free Balochistan demonstration against Pakistan (DharmaOrg / Public Domain)

**Gwadar, Pakistan.** The central port city of the CPEC project (umairadeeb / CC BY 4.0)

kistan Economic Corridor (CPEC) project, Beijing is trying to help Pakistan reach those coal riches. This may not sit well in Thar, a poor, bone-dry region in a province that houses small networks of Sindh nationalists, some of whom advocate separation from Pakistan. I'm not saying we could see a Baluchistan-like insurgency — separatist sentiment in Sindh pales in comparison to Baluchistan — but if Pakistan, with China's help, were to start moving on the Thar coal riches, there could certainly be a rise in tensions within local communities.

**FSR:** If billionaire investments do not suffice to solve the energy crisis, how can the international community, and particularly the United States, assist Pakistan to improve its energy problem?

**MK:** There are certainly measures that the international donor community can take, but ultimately they can only be tactical and not long-term fixes. Above all, international support can — as it has in the past — help pay for critical repairs to old and poorly maintained energy infrastructure. This can go a long way toward decreasing Pakistan's supply-demand gap by reducing line losses and making the generation, transmission, and distribution sides more efficient. But at the end of the day, I'd argue that only Pakistan can address its energy problems in a lasting, meaningful way. It will need to bring more order to the institutional aspects of the energy sector so that you don't have so many different energy-focused entities working at cross purposes. In an ideal world, you'd establish a central energy ministry — which Pakistan has never had — to oversee policy and management. Pakistan will also need to achieve a less expensive, more diverse energy mix, so that it doesn't overly rely on pricey hydrocarbon imports from the Middle East, as it does today.

## Michael Kugelman

Michael Kugelman is Deputy Director for the Asia Program at the Woodrow Wilson Center and is also the Center's Senior Associate for South Asia. He is responsible for research, programming, and publications on South Asia. His specialty areas include Afghanistan, Bangladesh, India, Pakistan, and U.S. relations with each of them. His recent projects have focused on India's foreign policy, U.S.-Pakistan relations, India-Pakistan relations, the war in Afghanistan, transboundary water agreements in South Asia, and U.S. policy in South Asia. He is a regular contributor to publications that include *Foreign Policy* and *Foreign Affairs*.

> The need is to address the issue and to facilitate investments in good teams of entrepreneurs that have the potential of becoming sustainable enterprises

**Speakers** at the High-level Dialogue on Trade and the Digital Economy in Africa panel during Africa eCommerce Week 2018 (Gleestitch Studios / CC BY-SA 4.0)

# Digitization and the Future of Trade

## A Conversation with Martin Labbé

Interviewed by FSR Staff

**Fletcher Security Review:** Digitization has been making big waves in the global economy and technology is more relevant than ever. Cross border e-commerce has become a key element of global economic activity and new business models are dependent on movement of data across borders. In other words, “Digital Trade” is shaping the fourth industrial revolution. The International Trade Centre (ITC) has been playing an important role in ensuring that the developing world reaps all the benefits of this growing trend. Could you talk a little bit about the ITC’s work in this area and give us a background of trends in digital trade from the organization’s lens?

**Martin Labbé:** The International Trade Centre (ITC) is an agency set up jointly by the United Nations (UN) and the World Trade Organization (WTO) and its key objective is to provide countries with trade-related technical assistance. We work with small and medium enterprises (SMEs), national chambers of commerce, export promotion agencies, and ministries of trade in developing countries. We primarily work in Africa but also to some extent in South Asia, the Pacific, and the Caribbean. Historically, we have been engaged in supporting the development of exports in such sectors as agriculture, handicrafts, and tourism.

In 2005, we started getting engaged in several projects on information and communication technologies (ICT) for development. These were the days when we saw the first wave of tech infrastructure being rolled out in Africa. Mobile penetration in Africa was growing, albeit at a small level. We saw a lot of potential in using mobile technologies to enable farmers, SMEs, and women-led businesses to transact. A lot of these projects never went beyond the pilot phase because of a lack of financial capacities or of people on the ground to turn them into successful, sustainable initiatives.

MINISTÉRIELLE DE L'OMC
BUENOS AIRES - ARGENTINA 2017
WTO OMC
BUENOS AIRES 2017
CONFERENCE
BUENOS AIRES - ARGENTINA 2017
WTO MINISTERIAL CONFERENCE
ARANCHA GONZÁLEZ
EXECUTIVE DIRECTOR, INTERNATIONAL TRADE CENTRE
GUÐLAUGUR ÞÓR ÞÓRÐARSON
FOREIGN MINISTER, ICELAND

**Executive Director of the ITC** Arancha González (center) speaks at a WTO conference (World Trade Organization / CC BY-SA 4.0)

***Jumia*** presents at the 2017 Web Summit (Stephen McCarthy / CC BY 4.0)

After that, we started to explore other possibilities for making Africa more tech-savvy. In 2010, our focus shifted to supporting the information technology (IT) sector in developing countries with the belief that they will be better at supporting the digitization in their countries. We did projects in Bangladesh, Kenya, Uganda, and Sri Lanka, some of which are still ongoing. Our key objective was to develop a new kind of exports – exports that would be happening not in containers and parcels, but through data and fiber optic cables; all of which today are a big part of the digital trade phenomena.

Around 2015, we saw another wave of tech-entrepreneurs and start-ups in the Silicon Valley and other advanced ecosystems, smaller and more fragile than SMEs, yet, with a potential to bring about change at a much larger scale than traditional SMEs could have. Commonly referred to as "unicorns," these start-ups like Spotify and Facebook were very successful in advanced countries, while their growth in Africa has been limited. The very few unicorns that have been able to scale up in the region are in fact non-indigenous companies. For instance, the largest player in the region, *Jumia*, was initiated by Rocket Internet, a German venture firm. As an e-commerce company, *Jumia* was first setup in Nigeria and then spread across the continent. It has been extremely successful in a variety of businesses: from delivery of consumer goods to meal delivery. We have also seen other investments coming in from Europe and elsewhere.

These three waves trace the trends in digital trade from ITC's lens: what ITC is interested in and supports through its projects.

**FSR:** It seems like the African region is at a significant disadvantage when compared to advanced countries and this points to a growing "digital divide." Further, this digital divide seems to exist not only among countries, but also within countries, i.e. between big and small companies. Is it fair to say that as global trade becomes more digitized, there will be "losers" and "winners"? What are the international community and the national governments doing to create a level playing field? And how do you think this problem can be solved?

**ML:** Overall, digital trade is growing rapidly and there certainly are a number of African success stories in say, financial technology. For instance, *Cellulant* in Kenya and other relatively small firms that we are working with, like *XENTE* in Rwanda and *Intouch* in Senegal.

**Senior government officials** from Kenyan Ministries of Education, of Science and Technology, and of ICT meet with UNESCO members and professors to discuss technology in education (CopyrightX Kenya / CC BY 4.0)

These are the firms that are contributing directly in development of digital trade in Africa and are indeed "winners." But then there are smaller players that are really struggling. Poor connectivity, problems with energy supply and fragmented markets are some of the factors creating the "losers" in Africa.

Digital trade has moved so rapidly that governments are struggling to catch up. It is often also noted that governments are not putting in place favorable regulations. For instance, some countries have been keen on imposing a tax on mobile money and social media. Such measures are counterproductive and slow down the growth of the digital economy. While this does not affect the larger international players directly, it certainly hurts the smaller businesses who don't have the same deep pockets to go through this difficult period.

But the situation is not so bad. In a welcome move by the WTO, over 70 countries have recently decided to resume work on e-commerce—an indication that the issue is being prioritized. Another interesting trend we see is the emergence of tech startups trying to make a social impact. A tech startup in Senegal, for instance, is providing a platform for fisherman to sell their fish directly to restaurants and private customers instead of selling it to middlemen. This is an intermediation dream that we have always sought to achieve. Yet again, scaling up is difficult. The key challenge is limited access to funding. This is not about access to finance or banks (this only matters for large firms), but about access to business angels and venture capital. There is almost no African venture capital. There is a lot of global venture capital and only 1 percent of it is going into Africa. As such, these startups struggle to survive and scale. At ITC, we are trying to facilitate this through deployment of angel networks in the region. In Gambia for instance, we are putting in place a business angel network together with the African Business Network. The idea is to replicate good practices coming from all African countries, in order to ensure that these entrepreneurs have access to capital and are able to become sustainable businesses, quickly. The need is to address the issue and to facilitate investments in good teams of entrepreneurs that have the potential of becoming sustainable enterprises. This is how you reduce the number of losers.

**FSR:** Could you give us a little bit of perspective on what these small businesses and budding startups that you engage with have to say about the issues they are struggling with, specifically in the context of government support?

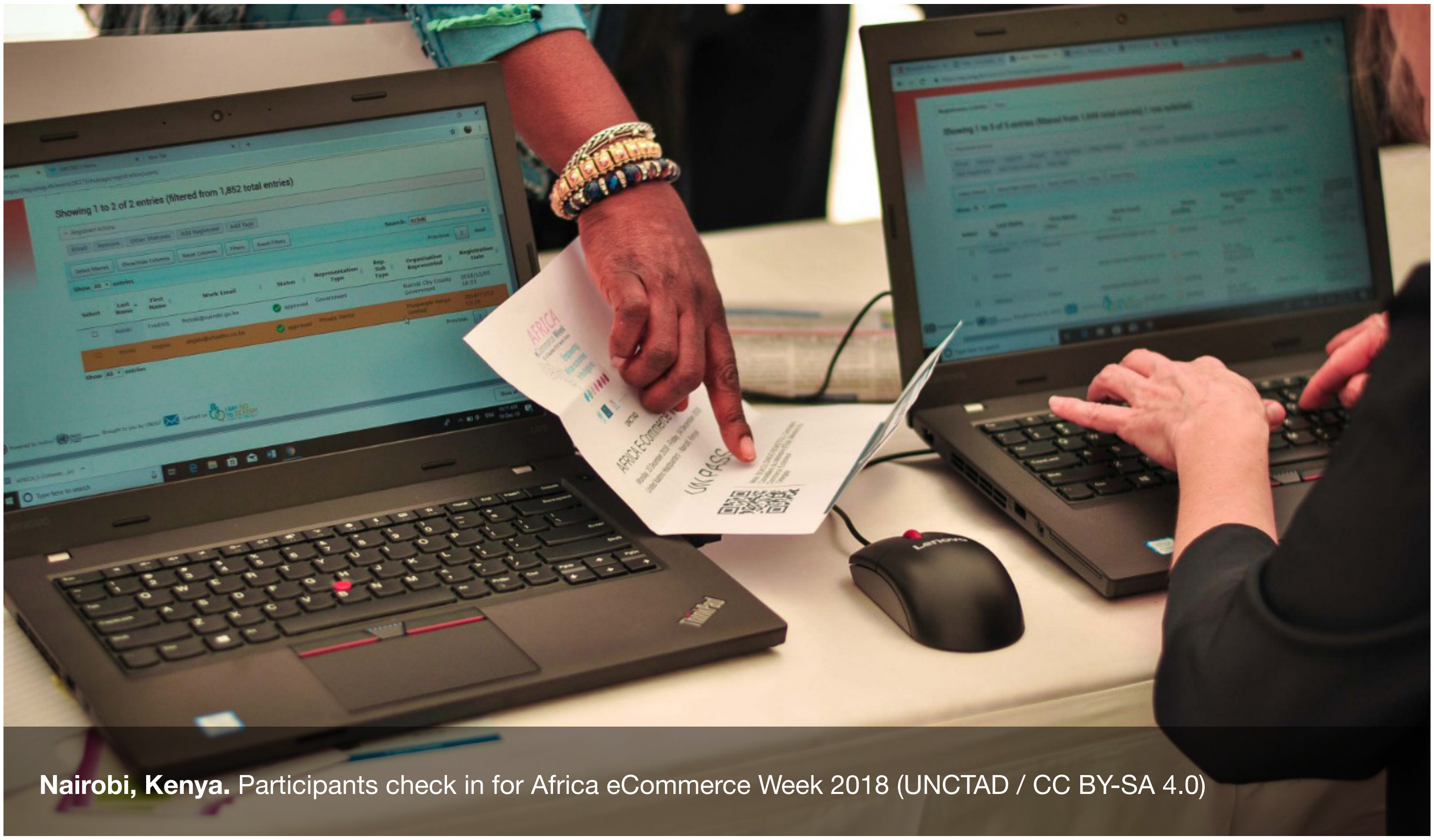
**ML:** Recently, we had a group of startups joining our executive director in Nairobi at the e-commerce week organized by UNCTAD. We asked them if there was anything they wanted us to share with their governments. The e-commerce startups provided us a comprehensive list of challenges they face. The key issues were those related to high cost of internet services/data, poor Infrastructure like road transport, unreliable electricity supply, and unreliable postal services that make online shopping significantly more difficult and less affordable. What also bothered them were data security and mistrust issues. For instance, in countries like Uganda and Nigeria people are very familiar with online scams and hesitate to provide their financial and other personal information online. Another issue raised was with respect to the challenge of including the digitally illiterate people who struggle to interact directly with businesses online. In addition, a large segment of the African population is unbanked. E-commerce businesses often have to set up country-specific sites because of payment issues.

The non-e-commerce startups complained that most start-ups and SMEs were drowning in taxes even before they could grow, if they play by the book. The Ugandan government has for instance recently implemented taxes on social media — USD 20/year — and mobile money — a 1 percent tax on transactions. Small businesses having to pay taxes on top of data at a very high cost is a real issue. Further, tax holidays which are given to foreign businesses in Uganda are not given to local businesses.

To conclude, these startups said that it was very hard to work with the government, given that its terms and conditions favored larger corporations. And then, there is the issue of corruption, closely tied to the failure of regulatory policies.

**FSR:** When you carry out projects in developing countries, are the governments receptive and open?

**ML:** Being a UN organization, it is very important for us to engage with the governments. We are not there to alienate the government, nor are we there to teach lessons. But we have to be wary that we are talking about new age, cutting-edge issues here at a point where these countries still have a wide range of pressing issues to deal with. Some of these countries have seen their populations double in the last ten years. They are facing massive infrastructure problems and high levels of un-



**Nairobi, Kenya.** Participants check in for Africa eCommerce Week 2018 (UNCTAD / CC BY-SA 4.0) employment. So talking about digitization may not be at the very top of their priorities. Yet, there are African countries that are taking a lead on this. Rwanda for instance, even as a Least Developed Country, has been extremely proactive in developing its digital economy. They have a very well structured and articulate approach for development of their tech sector and all government players are actively involved in supporting emerging entrepreneurs. This is what is also required in the rest of Africa—having a systemic approach to build the right infrastructure. For this to materialize, a number of players will need to come together. If there are tech startups and hubs but the government is not engaged, banks are not playing their role, there is no alternative funding source or academia is looking elsewhere—the ecosystem will be dysfunctional.

**FSR:** What about the emerging economies like China or India? Where do they stand in this digital trade architecture?

**ML:** The situation is totally different in India and China. India has been able to turn its IT and business process outsourcing (BPO) business into a USD 100 billion revenue stream. They have been able to build massive companies like Tata Consultancy, WIPRO, Cognizant, and others that have become extremely successful. China is another great example. It started primarily with the exports of hardware and then brands like Huawei and Xiaomi became market leaders and world number one handset manufacturers. Today, China is leading not just the hardware side of the business, but also leading innovation. So, it is a totally different scenario in the large emerging economies. Scale has been really important: it has pushed countries like China into a virtuous circle, whereas the lack of scale in Africa pushes those companies in a vicious cycle as they continue to struggle to increase their footprint. We are trying to fix this through private-public dialogues as well as by working with intermediaries.

**FSR:** In the larger scheme of things, where do you think Africa stands and how long a road is left to travel to reach where it ought to be, given all the complications you talk about?

**ML:** In 2005, the mobile penetration rate was below 30 percent, restricted largely to voice and SMS and maybe broadcast of information, but that is it. Since then, within so little time, we have been able to get to 100 percent penetration in many African countries. We have seen infrastructure being rolled out, the cost of data going down, and more and more people having access to smartphones for a cost as little as USD 50 which was a cost of a simple feature phone back in 2005. So there have been really massive, encouraging changes. Many countries like South Africa, Kenya, Uganda, Senegal, Ivory Coast, and Nigeria are taking advantage of opportunities in Sub-Saharan Africa. Further, policy efforts are being made at the continent level to improve the free flow of people and merchandise across African countries. There is a willingness to follow the example of what is happening in Europe and elsewhere in the world. The recently concluded Continental Free Trade Agreement is a great example of this.  New technology continues to roll out and an increasing number of players are deploying faster and ever more powerful technologies on the continent. There are investments being made to support tech entrepreneurship. These are all positive trends that make me really optimistic. If the governments continue with their integration efforts to create a single African market, there will also be a single digital African market. Once the desired framework is put into place, entrepreneurs will independently navigate the space. I would say, in the next five years, we will have travelled a great distance. We are in fact just at the beginning of a very positive trend.

## Martin Labbé

Martin Labbé is the Tech-Sector Development Coordinator at the International Trade Centre and the Program Manager for Netherlands Trust Fund IV (NTF IV), a USD 10 million Export Sector Competitiveness Program. He manages NTF IV Uganda and NT IV Senegal tech-sector development projects, working closely with IT sector associations & tech hubs, SMEs and tech startups to support the internationalization of the local digital economy. He has been actively involved in designing and managing several online and offline B2B business-development and marketing activities in developing countries and transition economies as well as training small- and medium-sized enterprises (SME) on technology and trade, with a focus on e-commerce.

# Photo Credits

Cover - Keifer Chiang | Contents - Earth Observatory, NASA | 5 - The Russian Presidential Press and Information Office (bit.ly/2VEjPSs) | 7 - Vitaly V. Kuzmin (bit.ly/2GXUmd4) | 8 - Ohnedich (flic.kr/p/272G1pV) | 9 - Vitaly V. Kuzmin (bit.ly/2GZw1oy) | 10 - Vitaly V. Kuzmin (bit.ly/2VKQPZa) | 11 - The Russian Presidential Press and Information Office (bit.ly/2H1XVAj) | 12 - The Russian Presidential Press and Information Office (bit.ly/2ZYnbig) | 15 - National Nuclear Security Administration | 16 - White House Photographic Office | 17 - Phoenix7777 (bit.ly/2JhcHWa) | 18 - The Russian Presidential Press and Information Office (bit.ly/2JAEwZ9) | 19 - Staff Sgt. N.B. | 24 - Cherie Cullen | 26 - Senior Master Sgt. C.R. | 29 - David James Paquin | 30 - IceUnshattered (bit.ly/2Jf1zJF) | 31 - Petty Officer 3rd Class Shawn Handley | 32 - Antônio Milena (bit.ly/2PYU4qF) | 33 - Sgt. Salvador R. Moreno | 35 - Zana Omar | 37 - Tech. Sgt. Michael R. Holzworth | 39 - 椎林 隆夫 (bit.ly/2WnoWn3) | 41 - Mikhail Metzel (bit.ly/2DLrrby) | 42 - U.S. Navy Petty Officer 1st Class Daniel Hinton | 45 - U.S. Office of the Director of National Security | 47 - Pete Souza | 49 - BalticServers (bit.ly/2gdndAe) | 51 - James Tourtellotte | 53 - Kevin Tao (flic.kr/p/G93fQg) | 54 - Leena Hietanen (bit.ly/2vT7Phi) | 55 - The Russian Presidential Press and Information Office (bit.ly/2He0yiH) | 56 - Kosandr (bit.ly/2JuPjUw) | 58 - Kevin Tao (flic.kr/p/G93fMF) | 61 - Patrick Nouhailler (flic.kr/p/ecSo9T) | 63 - National Security Agency | 65 - Web Summit (flic.kr/p/2bmG1jP) | 67 - United States Secret Service | 68 - Kemberly Groue | 69 - U.S. Department of Homeland Security | 70 - NASA | 72 - Ken Lund (flic.kr/p/nMygXZ) | 73 - Alex R. Lloyd | 75 - ICAN Australia (bit.ly/2vTECD8) | 77 - CTBTO (flic.kr/p/8vx5CR) | 78 - SrA. Ian Dudley | 79 - NASA | 81 - Lance Cpl. Thomas Mudd | 83 - Vif12vf (bit.ly/2VW4vk1) | 84 - U.S. Embassy Pakistan (flic.kr/p/dwTvSc) | 85 - DharmaOrg | 86 - umairadeeb (flic.kr/p/Q9mZYD) | 87 - Gleestitch Studios (flic.kr/p/2dFyxVX) | 88 - World Trade Organization (flic.kr/p/21onVWU) | 89 - Stephen McCarthy (flic.kr/p/21iEV9V) | 90 - CopyrightX Kenya | (bit.ly/2JgOkIo) | 91 - UNCTAD (flic.kr/p/2duLXBg)

CC BY 4.0 - creativecommons.org/licenses/by/4.0
CC BY-SA 4.0 - creativecommons.org/licenses/by-sa/4.0
CC BY-ND 4.0 - creativecommons.org/licenses/by-nd/4.0
CC BY-NC 4.0 - creativecommons.org/licenses/by-nc/4.0
CC BY-NC-SA 4.0 - creativecommons.org/licenses/by-nc-sa/4.0
CC BY-NC-ND 4.0 - creativecommons.org/licenses/by-nc-nd/4.0

FLETCHER SECURITY REVIEW

OMNIBUS SECURITAS

The Fletcher Security Review | Tufts University

www.fletchersecurity.org