The Strategist

Texas National Security Review: Volume 4, Issue 3 (Summer 2021)
Print: ISSN 2576-1021 Online: ISSN 2576-1153

CYBER RISK ACROSS THE U.S. NUCLEAR ENTERPRISE

Herbert Lin

LIVE ATTACKS
ATTACKER IP
ATTACKER GEO
TARGET GEO
ATTACK TYPE
PORT
216.218.206.73 Fremont, US Kirksville, US unknown 1434
218.26.79.228 Taiyuan, CN Lynnwood, US unknown 50864
46.151.209.24 Riyadh, SA Riyadh, SA unknown 137
46.151.215.168 Riyadh, SA Riyadh, SA unknown 137
61.147.103.166 Nanjing, CN Roseville, US ms-sql-s 1433
61.147.103.166 Nanjing, CN Roseville, US ms-sql-s
61.147.103.166 Nanjing, CN

As the United States embarks on an effort to modernize many elements of its nuclear enterprise, it needs to consider how dependencies on modern information technologies could lead to cyber-induced failures of nuclear deterrence or to nuclear war. The Biden administration has an opportunity to address issues of cyber risk across the entire nuclear enterprise in ways that previous administrations have not.

Over the past year, a number of seriously consequential cyber attacks against the United States have come to light. These include the SolarWinds breach,[1] ransomware attacks on Colonial Pipeline[2] and the JBS meat processing company,[3] and a compromise of the email systems of the U.S. Agency for International Development.[4] U.S. officials have indicated their belief that Russia either sponsored these attacks or at least tolerated the activities of the Russia-based hacker groups responsible for them.

That such attacks have happened at all raises important and disturbing questions about risks to the increasing U.S. dependency on information technology, including that of nearly every aspect of America's nuclear force management, from stockpile management to launch. These risks suggest that American nuclear forces may be far more vulnerable to cyber disruption, destruction, and corruption than policymakers realize.

Many of the existing components of the U.S. nuclear enterprise — that is, the entire array of activities and operations that have some significant connection to any aspect of nuclear explosive devices (usually known as nuclear weapons), whether in production, acquisition, operations, organization, or strategy — were developed before the Internet of Things, the World Wide Web, and mobile computing and smart cell phones became ubiquitous throughout society. Today, the United States is embarking on an effort to modernize many elements of its nuclear enterprise,[5] and, unlike in the past, cyber issues will be an increasingly important aspect of that effort. How, if at all, could dependencies on modern information technologies lead to cyber-induced failures of nuclear deterrence or result in a nuclear war? This is the question that motivates this essay.

A cyber-enabled world affords many benefits to individuals, businesses, and society at large, as well as to the military. U.S. military forces are unparalleled in the world, in part because of their use of information technology. But the growing use of modern information technologies has a downside as well, and where nuclear weapons are concerned, it behooves us to examine that downside and to mitigate it where possible.

The bottom line? Cyber risks across the nuclear enterprise are poorly understood. A number of aspects of the nuclear modernization effort are likely to exacerbate, rather than mitigate, these risks. The Biden administration will have to find ways to effectively manage tensions between adopting new nuclear capabilities and increasing cyber risk. Senior U.S. decision-makers are aware of these problems to some extent, but they face two important challenges. The first is that limiting cyber risk may require making some hard choices about what nuclear capabilities to give up. The second is to close the large gap that exists between that awareness and remedial actions being taken on the ground.

[1] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," *NPR*, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[2] Geneva Sands and Arlette Saenz, "Criminal Group Originating from Russia Believed to Be Behind Pipeline Cyberattack," *CNN*, May 9, 2021, https://www.cnn.com/2021/05/09/politics/colonial-pipeline-cyberattack-restart-plan/index.html.

[3] Bill Chappell, Dina Temple-Raston, and Scott Detrow, "What We Know About the Apparent Russian Hack Exploiting a U.S. Aid Agency," *NPR*, May 28, 2021, https://www.npr.org/2021/05/28/1001237516/what-we-know-about-the-apparent-russian-hack-exploiting-a-u-s-aid-agency.

[4] David E. Sanger and Nicole Perlroth, "Russia Appears to Carry Out Hack Through System Used by U.S. Aid Agency," *New York Times*, May 28, 2021, https://www.nytimes.com/2021/05/28/us/politics/russia-hack-usaid.html.

[5] *Nuclear Posture Review*, Department of Defense, 2018, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

Modernizing the U.S. Nuclear Enterprise

The U.S. nuclear enterprise has many elements, including nuclear delivery platforms and missiles, and a nuclear command, control, and communications (NC3) infrastructure (all of which are operated by the Department of Defense), as well as the Department of Energy nuclear weapons complex that is responsible for the weapons themselves. Further, the 2018 *Nuclear Posture Review* calls for the United States to modernize its nuclear weapons and to acquire new nuclear delivery platforms and missiles as well as a new NC3 infrastructure to meet the command-and-control needs of the emerging environment of great-power conflict. As this effort is launched, the U.S. government will have to pay close attention to managing cyber vulnerabilities that are likely to arise in every element of the nuclear enterprise.

The Nuclear Weapons Complex

The nuclear weapons complex refers to activities and operations associated specifically with the life cycle of the explosive devices themselves, as opposed to the platforms that carry them or how they might be used. It works to ensure the safety, security, and effectiveness of the U.S. nuclear weapons stockpile.

Since the Cold War's end, the United States has not produced an entirely new nuclear explosive device and has abided by a voluntary moratorium on nuclear testing. Periodic nonnuclear testing and analysis of the test results is the most common way to ensure the continuing reliability of old devices. In addition, a number of Department of Energy facilities continue to explore the basic physics underlying nuclear weapons. Computer simulations of nuclear explosive phenomena, combined with basic physics and data from past nuclear tests and data collected from current nonnuclear testing, are used to generate the scientific basis upon which judgments and assessments about the existing nuclear stockpile can be made. Through this process, each nuclear weapon in the U.S. nuclear arsenal is assessed to determine its reliability and to detect and anticipate any potential issues that may come from aging.[6] Any problems that are found result in corrective actions whose efficacy must be ascertained, again largely through computer-based simulations.

Given the extreme dependence of the stockpile on computing, maintaining the security of the computer programs and databases involved is obviously necessary. Subtly and surreptitiously altered programs or databases could corrupt the basis upon which scientists make their judgments about the nuclear stockpile. The most difficult-to-address aspect of maintaining the confidentiality and integrity of programs and databases is the insider threat — the concern that a trusted insider with all of the necessary clearances goes rogue and proceeds to make unauthorized changes. Many safeguards are in place to defend against the insider threat, which the laboratories take very seriously.

Another possible concern about cyber security in the nuclear weapons complex was raised by the SolarWinds incident in December 2020.[7] As of this writing, the Department of Energy has reported that "the malware has been isolated to business networks only, and has not impacted the mission essential national security functions of … the National Nuclear Security Administration."[8] It has also disconnected all software identified as being vulnerable to this attack from the Department of Energy network. However, many cyber security specialists have found, through experience, that organizational claims that business networks are kept entirely separate from mission-critical networks are often not reflected in reality. Such networks are not actually completely separate, and even when they are "air-gapped," human carelessness often enables adversaries to jump the gap. And, since the events of the SolarWinds incident are still being revealed, some vulnerable software may still be running on the Department of Energy network.

The Energy Department also depends on computer-controlled fabrication machinery that shapes various components of nuclear weapons, such as the high-explosive components used to compress fissile material to critical mass. But because the shapes must be precisely machined to very tight tolerances, the equipment used to fabricate charges is necessarily controlled by computers. Although these computers would not be connected directly to the internet, it must be possible to program them, and they must access data from appropriate databases to fabricate the components in question.

[6] "Maintaining the Stockpile," Department of Energy, National Nuclear Security Administration, accessed June 10, 2021, https://www.energy.gov/nnsa/missions/maintaining-stockpile.

[7] Bill Chappell, Greg Myre, and Laurel Wamsley, "What We Know About Russia's Alleged Hack of the U.S. Government and Tech Companies," *NPR*, Dec. 21, 2020, https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little.

[8] "DOE Update on Cyber Incident Related to SolarWinds Compromise," U.S. Department of Energy, Dec. 18, 2020, http://www.energy.gov/articles/doe-update-cyber-incident-related-solar-winds-compromise.

Compromising these programs or data could cause the components to be fabricated in ways that are slightly off from the specification. Such imperfections would likely be caught in subsequent inspections, but their deliberate introduction into the fabrication process would be a definite minus for quality control.

Finally, there are cyber threats to nuclear weapons associated with the electronics they contain. For example, the triggering of a nuclear explosion requires a number of events to occur in a precisely timed sequence. Electronic mechanisms play a key role in orchestrating that sequence. The integrity of the supply chain — from the initial fabrication of these components to assembly and integration into the final weapon that enters the arsenal, along with any necessary programming — must thus be assured, as a vulnerability could be introduced at any point in this chain.

Nuclear Delivery Systems and Platforms

Nuclear weapons are delivered to their targets by airplanes and missiles. This includes both ballistic and cruise missiles today, and possibly hypersonic missiles in the future. Missiles themselves may be carried on weapons platforms, such as submarines or bombers. Airplanes, submarines, and missiles all rely on embedded computer systems to operate properly. Their survivability in the face of attack and their effectiveness in combat may also depend on computer systems (and networks) that are a part of their combat and logistical support infrastructure.

The nuclear modernization program calls for the country's aging nuclear platforms and delivery systems to be replaced by entirely new intercontinental ballistic missiles, cruise missiles, bombers, and missile-carrying submarines. Additionally, the F-35 is expected to replace the F-15 and F-16 as the dual-capable aircraft (i.e., capable of carrying both conventional and nuclear munitions) in the NATO theater.

As is the case with all new platforms and delivery systems, these new systems will depend on computers and software to achieve their performance goals. For example, the F-35 will require at least 8 million lines of software code.[9] This software will support the F-35 in a variety of missions, including air-to-air combat; air-to-ground attack; electronic attack; and intelligence, surveillance, and reconnaissance. Computers will also control key aspects of the F-35's stealth capability. Finally, the F-35 has a sophisticated computer-based logistics support system to sustain and repair the airplane at lower cost and more rapidly than would otherwise be possible. Similar considerations will affect the new B-21 and the new Columbia-class ballistic missile submarine. Computers will be intimately involved in coordinating all of the electronic activity on board these platforms, which will touch navigation, propulsion, sensor systems, fire control systems, and so on.

Exploitation of cyber vulnerabilities in nuclear delivery systems could prevent or impede the proper delivery of a weapon to its target. For example, an airplane carrying a nuclear gravity bomb might not be able to release it at the appropriate time should the computers controlling the weapon's release be rendered unavailable. An airplane carrying a nuclear weapon might not be able to take off because the onboard computer systems are constantly rebooting.[10] Stealth aircraft almost certainly achieve some of their undetectability to radar due to active measures that are controlled by computer. The same may be true of ballistic missile submarines trying to evade being detected by active sonar. A small unauthorized change to a computer program could make a stealth aircraft more visible to radar or a submarine noisier in the ocean.[11]

Department of Defense weapons systems and networks also rely on components and services that the department does not fully control. For example, airplanes, submarines, and missiles use a variety of electronic components and software from myriad suppliers, any of which is a potential access path to the system — the so-called supply-chain vector for cyber attacks, as demonstrated in the SolarWinds hack.[12] The Defense Department also engages in a large volume of electronic commerce with a variety of private-sector commercial entities to supply its substantial logistical needs. The integrity and availability of internal Defense Department systems and those of commercial providers are thus essential aspects of the department's operations. Compromising those functions could impact readiness. Lastly, the connections between Defense

[9] "F-35 Software Development: A Digital Jet for the Modern Battlespace," Lockheed Martin, accessed June 10, 2021, https://web.archive.org/web/20210123100734/https://www.f35.com/about/life-cycle/software.

[10] Clay Dillow, "Only One of Six Air Force F-35s Could Actually Take Off During Testing," *Fortune*, April 28, 2016, https://fortune.com/2016/04/28/f-35-fails-testing-air-force/.

[11] On stealth aircraft radar visibility, see Mingxu Yi, Lifeng Wang, and Jun Huang, "Active Cancellation Analysis Based on the Radar Detection Probability," *Aerospace Science and Technology*, no. 46 (October-November 2015): 273–81, https://doi.org/10.1016/j.ast.2015.07.018.

[12] "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," FireEye Threat Research Blog, December 13, 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html.

Department networks and the broader internet provide multiple access paths through which weapons systems and command, control, and communications (C3) networks can potentially be compromised. Disconnecting weapons systems from U.S. military systems and networks sometimes helps to limit adversary access, but it does not guarantee that adversaries cannot reach them because they could still gain physical access to the systems.

A recent report from the U.S. Government Accountability Office probed cyber vulnerabilities in U.S. weapons systems and arrived at some worrisome conclusions. This report noted that the Defense Department routinely finds mission-critical cyber vulnerabilities during operational testing of weapons systems that are under development, pointing out that "using relatively simple tools and techniques, testers were able to take control of systems and largely operate undetected."[13] Even worse, the Government Accountability Office found that the discovered vulnerabilities represented only a fraction of total vulnerabilities because not all weapons systems were tested; Defense Department testing did not reflect the full range of cyber threats that a sophisticated adversary might deploy against the weapons systems being tested; thorough review was sometimes impossible because the department was denied access to review proprietary software; and certain tests were not performed because cyber security testing would have interfered with operations.

Nuclear Command, Control, and Communications

The NC3 system supports both ongoing and episodic functions and consists of five key elements. *Nuclear planning* refers primarily to developing options for the use of nuclear weapons, both preplanned options in anticipation of certain contingencies and ad hoc options to address unforeseen contingencies. *Force management* is, among other things, the function associated with ensuring the safety, surety, security, and reliability of these weapons and their associated support systems. *Situation monitoring* relates to the collection, maintenance, assessment, and dissemination of information on friendly forces; adversary forces and possible targets; emerging nuclear powers; and military, political, environmental, and other events. Situation monitoring also includes tactical warning and attack assessment — the ability to detect and characterize an attack that has been launched against the U.S. homeland. *Nuclear decision-making* involves the use or movement of nuclear weapons or the execution of other nuclear control orders. It may, in crisis situations, entail consultations between the president of the United States and others, including foreign leaders in allied nations, domestic leaders, trusted civilian advisers, senior U.S. military leaders, social and traditional media outlets, and possibly adversary leaders as well. *Force direction* relates to the implementation (preparation, dissemination, and authentication) of decisions regarding the execution, termination, destruction, and disablement of nuclear weapons. It is supported by much of the physical infrastructure of the NC3 system.

The NC3 system includes infrared satellites and ground-based radars that provide information about ballistic missile launches around the world; space-based detection capabilities that identify and geo-locate above-ground nuclear explosions; a variety of fixed and mobile facilities to interpret sensor information, formulate presidential orders, and pass those orders to the nuclear forces for implementation; and multiple wired and wireless communications capabilities to transmit orders and to receive information relevant for decision-making. Some components of this infrastructure have undergone a substantial evolution over the last 30 years, with, for example, new communications systems being added. Because a common underlying technical architecture has not existed to support the overall system, each new component has been pursued as a standalone. Integrating new components into an old overall system has necessitated new hardware, new software, and new operating procedures and practices.

In the opinion of many senior military leaders, the cyber threat to today's NC3 system is "fairly minimal."[14] This is fortuitous and is due to the age of the system and the consequent fact that the system is largely disconnected from the rest of the military and civilian world. That is, today's system is more secure because it is not connected to other parts of the world from which various cyber threats could emanate. The minimal nature of the cyber threat against today's NC3 system is not due so much to the age of its components, but rather to the fact that even newly modernized components have been plugged into the old point-to-point

[13] "GAO 19-128: Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities," U.S. Government Accountability Office, Oct. 9, 2018, 21, https://www.gao.gov/products/GAO-19-128.

[14] See, for example, testimony of Gen. John Hyten: "U.S. Strategist Command and U.S. Northern Command SASC [Senate Armed Services Committee] Testimony," March 1, 2019, available at U.S. Strategic Command, https://www.stratcom.mil/Media/Speeches/Article/1771903/us-strategic-command-and-us-northern-command-sasc-testimony/.

hardwired architecture.

That said, America's NC3 system has not been entirely immune to threats that could have been caused by malevolent cyber actors. The history of U.S. nuclear command and control shows several false alarms indicating Soviet nuclear attack when no such attack was taking place.[15] NC3 for U.S. intercontinental ballistic missiles has also displayed electronic vulnerabilities: In 2010, launch crews in ground-based launch control centers lost contact with 50 nuclear-armed missiles for an hour in Wyoming because of an improperly installed circuit card.[16] None of these cases was, strictly speaking, caused by malevolent cyber actors. But they do demonstrate the potential dangers that could arise were such malevolent actors to target the NC3 system.

Other cyber threats to NC3 include a loss of confidentiality regarding deliberations and decisions. Most political leaders would prefer to keep their options open as they make momentous decisions. Revealing to the public or to foreign intelligence the substance of these deliberations is likely to increase pressure from one or another source to take a particular course of action. Nuclear planning and the stockpile stewardship program rely on a variety of databases and programs whose currency and integrity must be assured. Deliberate corruption of these databases or programs would inevitably lead to suboptimal outcomes in nuclear operations.

Substantial efforts are being and will be made to modernize the NC3 system. According to the Congressional Research Service, NC3 modernization is likely to include new early-warning radars, new infrared early-warning satellites, new communications satellites, and replacements for the E4-B airborne command posts and E6-B communications relay aircraft.[17] But just as importantly, new nuclear delivery systems and platforms will be "much more like all systems today, network connected. They'll be cyber enabled" and will have "some level of connectivity to the rest of the warfighting system," according to Werner J. A. Dahm, chair of the Air Force Scientific Advisory Board.[18] The significance of being "cyber-enabled" is hard to overstate. Adm. Cecil Haney, former commander of U.S. Strategic Command, testified in 2014 that "We are working to shift from point-to-point hardwired systems to a networked IP-based national C3 architecture."[19] The shift to "cyber-enabled" connectivity will mean a higher degree of interoperability among NC3 components, which will no longer be as constrained by hardware restrictions.

In March 2019, Gen. John Hyten, then-commander of U.S. Strategic Command, called the NC3 system resilient, reliable, and effective, but said that its functionality would be questionable in about a decade.[20] It is in this context that the 2018 *Nuclear Posture Review* specifically called attention to the need to modernize the NC3 system.[21] One reason is that space as a domain of military operations is much less of a sanctuary today than it was in the mid-1980s, the last time the NC3 system underwent significant modernization and change. A second reason is that potential adversaries are emphasizing the employment of limited nuclear strikes, making it necessary for the U.S. NC3 system to be resilient to such attacks. In such a scenario, nuclear weapon effects could potentially impair the theater elements of U.S. and allied NC3 systems, inhibiting early warning, sensors, multinational leadership conferencing, and prospective orders to theater-based nuclear forces.[22] Such effects could force the United States to conduct further nuclear operations, should they become necessary, in that degraded environment.[23] It is true that systems used primarily for NC3 purposes are designed to operate in a nuclear environment, but the fact remains that they have never been tested end-to-end in a true nuclear environment. Thus, unexpected problems of presently unknown magnitude are

[15] See, for example, Daryl G. Kimball, "Nuclear False Warnings and the Risk of Catastrophe," Arms Control Association, December 2019, https://www.armscontrol.org/act/2019-12/focus/nuclear-false-warnings-risk-catastrophe.

[16] Marc Ambinder, "Failure Shuts Down Squadron of Nuclear Missiles," *The Atlantic*, Oct. 26, 2010, https://www.theatlantic.com/politics/archive/2010/10/failure-shuts-down-squadron-of-nuclear-missiles/65207/.

[17] "Nuclear Command, Control, and Communications (NC3) Modernization," *In Focus*, Congressional Research Service, Dec. 8, 2020, https://fas.org/sgp/crs/nuke/IF11697.pdf.

[18] See Patrick Tucker, "Will America's Nuclear Weapons Always Be Safe from Hackers?" *The* Atlantic, Dec. 30, 2016, https://amp.theatlantic.com/amp/article/511904/.

[19] "Statement of Admiral Cecil D. Haney, Commander, United States Strategic Command," U.S. Senate Committee On Armed Services, 113th Congress, 2nd Session, Feb. 27 2014, https://www.hsdl.org/?view&did=751682.

[20] Hyten: "U.S. Strategist Command and U.S. Northern Command SASC [Senate Armed Services Committee] Testimony."

[21] Department of Defense, *Nuclear Posture Review*, 56.

[22] David A. Deptula and William A. LaPlante, with Robert Haddick, *Modernizing U.S. Nuclear Command, Control, and Communications*, Mitchell Institute for Aerospace Studies and the MITRE Corporation, February 2019, http://docs.wixstatic.com/ugd/a2dd91_ed45cfd71de2457eba3b-cce4d0657196.pdf, 27.

[23] John R. Harvey, "U.S. Nuclear Command and Control for the 21st Century", Nautilus Institute for Security and Sustainability, NAPSNet Special Reports, May 24, 2019, https://nautilus.org/napsnet/napsnet-special-reports/u-s-nuclear-command-and-control-for-the-21st-century/.

likely to appear.

The 2018 *Nuclear Posture Review* calls for U.S. leadership, including senior military commanders, to be able to communicate and share information across their command-and-control systems and to integrate nuclear and nonnuclear military planning and operations in the context of a nuclear attack. Further elaborating on this point, Hyten stated in February 2020 that NC3 and Joint All-Domain Command and Control are intertwined and that NC3 will operate in elements of Joint All-Domain Command and Control. According to Hyten, each has to inform the other.[24] Joint All-Domain Command and Control is the Department of Defense's concept to connect sensors and shooters from all military services into a single seamless network. Although strategic nuclear and tactical conventional military data flows are currently connected to some extent, conventional-nuclear integration would improve this connection considerably.

Separately, the *Nuclear Posture Review* also identifies adversary offensive cyber capabilities as creating new challenges and potential vulnerabilities for America's NC3 system. Although the NC3 system remains assured and effective today, additional steps will be needed to "address [future] challenges to network defense, authentication, data integrity, and secure, assured, and reliable information flow across a resilient NC3 network."[25]

Cyber Security and the Nuclear Modernization Program

Given the role of information technology in all elements of the nuclear enterprise, it is clear that cyber security will be an issue of critical importance in the government's nuclear modernization efforts. Not many specifics are available about the NC3 architecture, its individual components, or how the other elements of the nuclear enterprise will connect with NC3, since the modernization program has more or less just begun. But it is possible to offer a couple of high-level comments based on what is known today. First, technology and geopolitics drive rapid change in the threat environment. Thus, the 2018 *Nuclear Posture Review* calls for the U.S. nuclear enterprise to be capable of adapting at a similar pace. By definition, adaptation entails changing the requirements that the various elements of the U.S. nuclear enterprise must fulfil. Usually, such changes will involve adding new capabilities and, as discussed below, will most likely entail additional cyber risk as well.

Second, many elements of the modernization program are entirely new programs rather than upgrades of existing elements of the nuclear enterprise. Although the nuclear explosive devices themselves will not be new, the program calls for a new strategic bomber, a new intercontinental ballistic missile, a new missile-carrying submarine, and a new long-range cruise missile, all of which will have to be integrated with a new NC3 architecture, which itself will have a number of new components. Newness offers the advantage of rationalizing an architecture that is currently a patchwork of components and custom-made "point" solutions. At the same time, components, systems, and architectures are at their most vulnerable when new, because users have not yet had the opportunity to identify and fix the problems that inevitably accompany newness.

The significance of these two comments is most apparent in the context of modernizing NC3. Integrating conventional and nuclear warfighting operations will place much greater demands for functionality on a NC3 system than one that mostly supports nuclear functions for deterrence purposes. Indeed, providing new capabilities is one reason for embarking on a multi-billion-dollar NC3 modernization. Similar comments apply to the capabilities of new delivery systems, which will have to face threats to survivability that include and go beyond those faced today.

It is likely that the modernized NC3 system as proposed will be functionally more complex than the legacy system it replaces. That additional complexity will be at least as much of a driver of increased cyber vulnerability as the fact that NC3 will have additional connections to the outside world through a networked, IP-based national C3 architecture that is at the core of a broader, national command-and-control system. The same will be true of new platforms and delivery systems — if history is any guide, the software aboard them will be considerably more complex than earlier platforms and delivery systems.

These new capabilities will depend heavily on information technology. But more functionality in an information technology system always entails increased complexity of design and implementation of that system, all else being equal (most system designers and architects will attest to this truism). That is, at a given level of technological sophistication,

[24] Colin Clark, "Nuclear C3 Goes All Domain: Gen. Hyten," *Breaking Defense*, Feb. 20, 2020, https://breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.

[25] Department of Defense, *Nuclear Posture Review*, Feb. 1, 2018, 57.

more functionality means more complexity. An increase in the technological sophistication of software can break this link in the short term. For example, compilers that translate high-level languages into machine code enable the development of programs that are less complex and more easily understandable (at the source code level) for a given level of functionality (as defined by what the computer actually does at the machine code level). But in the absence of continuous increases in sophistication of software-building technology, functionality means more complexity.

Evaluating the security of a system becomes more difficult as the system grows in complexity because there are more interfaces, more options, more specifications and requirements, more modules, more code, more interactions with external entities, more users, and more human errors.

In his 1980 Turing Award lecture (in computer science, the equivalent of the Nobel Prize lecture), C. A. R. Hoare noted that "there are two ways of constructing a software design: One way is to make it so simple that there are obviously no deficiencies, and the other way is to make it so complicated that there are no obvious deficiencies."[26] These lessons have been taken to heart by cyber security analysts, who are virtually unanimous in their contention that system complexity is the enemy of cyber security. Greater system complexity generally means more places where flaws can be found — flaws that an adversary can exploit. Evaluating the security of a system becomes more difficult as the system grows in complexity because there are more interfaces, more options, more specifications and requirements, more modules, more code, more interactions with external entities, more users, and more human errors.[27]

The functional requirements of a system determine its architecture, which includes the key operational objectives of the system; the operational elements, tasks, and processes used to achieve those objectives; a high-level description of the types of information used and created; how and with what constraints information of various types must be exchanged; and the information flows in these processes. The architecture can be related to specific mission scenarios and functions and is the basis for understanding and prioritizing operational processes and information flows. And yet, in all domains of life, including military operations, the evidence to date is that the appetite for increased functionality afforded by information technology is unlimited. Users want new systems to operate faster and more accurately, to offer more options, to be more easily used, to be interoperable with one another, and to process more and different kinds of data. However, security, in and of itself, is not desirable to users. It is only desirable to the extent that it enables users to have the functionality they want when they are under attack. Thus, by not moderating their appetites for functionality, users are implicitly asking for — indeed, demanding — more complex systems.

These comments should not be taken to mean that all demands for functionality are inappropriate. But demands for functionality must be weighed against the security costs that increased functionality entails. The first reality of cyber security is that more functionality usually wins.

A second undeniable reality of cyber security is that putting in place cyber security measures inevitably increases inconvenience for users. Such measures often make the systems to which they are applied clumsy and awkward to use, presenting significant obstacles to getting work done. As a result, cyber security measures are all too often disabled or bypassed by users, not because they are lazy but because they want to do their jobs well and don't see adhering to security measures as contributing to that goal. The tension between usability and cyber security is a difficult problem to address. One approach to mitigate it is to implement security measures that have explicitly been designed and tested to reduce the "hassle factor," thus increasing the likelihood that users will refrain from bypassing them. Nonetheless, irreconcilable tensions will sometimes be encountered, at which point the only approach is to implement security measures that are more difficult to bypass.

[26] Charles Antony Richard Hoare, "The Emperor's Old Clothes," *Communications of the ACM* 24, no. 2 (February 1981): 75–83, February 1981, https://dl.acm.org/doi/10.1145/358549.358561.

[27] Bruce Schneier, "A Plea for Simplicity: You Can't Secure What You Don't Understand," *Schneier on Security*, Nov. 19, 1999, https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html; and Nancy Leveson, "An Engineering Perspective on Avoiding Inadvertent Nuclear War," Nautilus Institute for Security and Sustainability, NAPSNet Special Reports, July 25, 2019, https://nautilus.org/napsnet/napsnet-special-reports/an-engineering-perspective-on-avoiding-inadvertent-nuclear-war/.

Scenarios Involving Cyber-Driven Pathways to Nuclear Crisis

To illustrate what is at stake if cyber risks are not adequately addressed, below are several nuclear scenarios in which cyber attacks by one side on the other might have a real and tangible effect on the the likelihood of nuclear use.

A first scenario involves differing perceptions of cyber penetrations of NC3 during a nuclear crisis. Cyber attacks and cyber espionage/intelligence gathering (cyber exploitation) use the same penetration techniques and differ only in what they seek to accomplish. Thus, any given cyber penetration carries with it an unknown potential for both attack and exploitation. A cyber penetration from nation A detected in nation B's NC3 system could be part of a relatively benign attempt to gather intelligence. Or it could be the start of a serious cyber attack. It is impossible for nation B to know nation A's intentions before the payloads are executed. A worst-case assessment would regard A's penetration as the start of an attack on B's NC3 system.[28]

A second scenario could arise when a nation chooses to combine (that is, to entangle) nuclear C3 and conventional C3 functions on the same technology platforms and take advantage of the same command, control, and communications infrastructure for reasons of economy. During the initial stages of a conflict, nation A may target nation B's conventional C3 infrastructure for the understandable and militarily justified purpose of degrading B's conventional combat power. But if the technological infrastructure for both conventional and nuclear C3 is the same, such an attack could actually degrade B's nuclear C3 capabilities as well as give rise to concerns that A is deliberately trying to degrade B's nuclear capabilities preemptively.[29]

A third scenario stems from the fact that offensive cyber capabilities are usually concealed out of a concern that, if revealed, an adversary will be able to negate those capabilities.[30] If nation A is able to penetrate nation B's nuclear enterprise clandestinely, A has the advantage over B without B realizing it. In a crisis, A knows it has the upper hand over B and feels no need to refrain from escalation. However, B does not know about the penetration, and, believing itself to be as strong as it ever was, does not know that it would be wise to refrain from escalation. Each side's unwillingness to refrain from escalation creates more risk for the other side.

A fourth scenario has to do with using cyber attacks to damage an adversary's confidence in its nuclear capabilities. Seeking to compromise an adversary's nuclear deterrent and exploiting vulnerabilities in its supply chains, nation A places malware (or hardware vulnerabilities) on a number of nation B's nuclear delivery platforms. During an escalating crisis, A communicates to B what it has done and demonstrates that it has done so by providing clues that allow B to discover these vulnerabilities. A then informs B that it has done this on many more of B's platforms. B now must consider how to react as it tries to determine what is mere boasting and which of B's platforms have been genuinely compromised.

A fifth scenario involves social media corruption of the information ecosystem in which decision-makers receive and process information. Although today's decision-makers and political leaders continue to have access to their traditional sources of analyzed and verified information from their intelligence services, they also increasingly engage directly with a public information ecosystem, which includes major social media and internet search elements that are not subject to the requirement of serious verification or analysis. These leaders and decision-makers process information and make decisions in this partially corrupted information environment. Consider, for example, that social media is designed for short, simple messages (often audio or video) that lack context and authentication and are more likely to stimulate emotionally visceral reactions than analytical thought. Psychological evidence suggests that people systematically deviate from rationality when making decisions,[31] thus calling into question the rationality of decision-makers that is

[28] This scenario is also addressed in a U.S.-Chinese context in Ben Buchanan and Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis," *Texas National Security Review* 3, no. 4 (Fall 2020): 55–81, http://dx.doi.org/10.26153/tsw/10951. They also conclude that the risk of inadvertent escalation due to cyber capabilities in a future Sino-American crisis cannot be dismissed.

[29] This argument is elaborated in James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018): 56–99, https://doi.org/10.1162/isec_a_00320.

[30] The scenario is based on a discussion in Erik Gartzke and Jon R. Lindsay, "The Cyber Commitment Problem and the Destabilization of Nuclear Deterrence," in *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*, ed. Herbert Lin and Amy Zegart (Washington, DC: Brookings Institution Press, 2018).

[31] See, for example, Dan Ariely, *Predictably Irrational: The Hidden Forces that Shape Our Decisions*, Revised and expanded (New York: Harper Perennial, 2010); Daniel Kahneman, Paul Slovic, and Amos Tversky, eds., *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge: Cambridge University Press, 1982); Jonathan Baron, *Thinking and Deciding*, 4th ed. (Cambridge: Cambridge University Press, 2008); Robert B. Cialdini, *Influence: The Psychology of Persuasion*, rev. Ed. (New York, NY: Harper Business, 2006); and Thomas Gilovich, Dale W. Griffin, and Daniel Kahneman, eds., *Heuristics and Biases: The Psychology of Intuitive Judgment* (Cambridge: Cambridge University Press, 2002). A more popularized discussion of this phenomenon can be found in Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

assumed in classical deterrence theory. In particular, under stress, people are more likely to default to fast, intuitive, and reactive decision-making rather than slower, more reflective, and deliberate decision-making.[32] The former type of thinking would be particularly dangerous in a nuclear scenario involving the possibility of launch-on-warning and its highly stressful and exceedingly short timelines.[33]

Observations and Imperatives for Reducing Cyber Risk for the Nuclear Enterprise

The Biden administration has inherited a nuclear modernization program that has already begun to get underway in earnest. But it is not too late for it to consider and apply a number of observations and imperatives that should guide the program as it moves forward.

The most important observation is that vulnerabilities to adversary cyber operations against the nuclear enterprise are not limited to technical attacks on NC3 components. Cyber risks affect all elements of the nuclear enterprise, although some elements, such as the Department of Energy-operated nuclear weapons complex, appear to have a more robust cyber security posture than those operated by the Department of Defense. Accordingly, it is crucial that efforts to improve the cyber security of the nuclear enterprise include all of its elements and address both acquisitions and operations.

A second observation is that entangling conventional and nuclear systems, whether with regard to the NC3 system or weapons platforms, raises the risk of inadvertent nuclear escalation in times of conflict. It is undeniable that integrating nuclear and conventional systems confers operational and financial advantages in warfighting. For example, early warning satellites that signal the launch of nuclear intercontinental ballistic missiles can also identify the launch of shorter range tactical ballistic missiles used in conventional warfighting. But those advantages must be weighed against an increased possibility that cyber attacks directed against those systems will inevitably raise fears among U.S. decision-makers that their own nuclear systems are being compromised, especially if those cyber attacks are coming from another nuclear power.

A number of imperatives follow from this observation. First, in the interest of greater simplicity, and thus greater security and reliability, designers of modernized computer-driven systems — whether NC3 or weapons platforms — should moderate their appetites for increased functionality, especially when it comes to nonnuclear missions. A key first step would be to define the *minimum* essential core functionality for nuclear operations. For example, in the case of NC3, this minimum essential functionality would cover the most important functions of the "thin line." (The "thin line" of NC3 is commonly understood to be the part of NC3 minimally providing "assured, unbroken, redundant, survivable, secure, and enduring connectivity to and among the President, the Secretary of Defense, the CJCS [Combined Joint Chiefs of Staff], and designated commanders through all threat environments [including nuclear environments] to perform all necessary command and control functions."[34])

The minimum essential functionality required of NC3 might *not*, for example, include the capability for crewed bombers to report back to senior commanders on battle damage assessment or other reconnaissance information gathered during their flight, or to receive retargeting information while en route to their primary targets. However, some functionalities should be retained even if they add complexity. One example is the environmental sensing devices that prevent nuclear weapons from exploding until they have encountered the expected physical conditions of weapons delivery — an essential element of nuclear safety. The architects of the NC3 system will have to make dozens — if not hundreds — of judgments to define minimum essential functionality.

However defined, the minimum essential functionality should be the basis for developing a relatively simple working system onto which additional functionality could be added. In addition, it could be embodied in an entirely independent backup system for NC3 to provide that core functionality should the primary systems be compromised.

The second imperative is that, given the role of nuclear weapons as "the *foundation* of our strategy

[32] See, for example, Jonathan St. B. T. Evans and Jodie Curtis-Holmes, "Rapid Responding Increases Belief Bias: Evidence for the Dual-Process Theory of Reasoning," *Thinking & Reasoning* 11, no. 4 (2005): 382–89, https://doi.org/10.1080/13546780542000005.

[33] Danielle Jablanski, Herbert S. Lin, and Harold A. Trinkunas, "Retweets to Midnight: Assessing the Effects of the Information Ecosystem on Crisis Decision Making Between Nuclear Weapons States," in *Three Tweets to Midnight: Effects of the Global Information Ecosystem on the Risk of Nuclear Conflict*, ed. Harold A. Trinkunas, Herbert S. Lin, and Benjamin Loehrke (Stanford, CA: Hoover Institution Press, 2020), 1–16, available at https://www.hoover.org/sites/default/files/research/docs/trinkunas_threetweetstomidnight_1-16_ch.1.pdf.

[34] *Nuclear Matters Handbook 2020*, Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, 26, https://fas.org/man/eprint/nmhb2020.pdf.

to preserve peace and stability,"[35] the network infrastructure built to support conventional-nuclear integration should prioritize the needs of the nuclear enterprise first. This goal will be difficult if, as is currently planned, NC3 acquisition will be controlled by the services rather than by U.S. Strategic Command. Service acquisition agencies are likely to give priority to the needs of their warfighting elements, which are, for the most part, nonnuclear. The fact that U.S. Strategic Command has a voice in making decisions about dual-capable elements of NC3 is a positive step. Nevertheless, the fact remains that system requirements will be negotiated between U.S. Strategic Command and the service acquisition agencies. Under such circumstances, it is usually the party with the actual acquisition authority to allocate budgets that benefits from the Golden Rule: Whoever has the gold makes the rules. In other words, because they control the money, the service acquisition authorities are in a better position and more likely to make a host of "smaller" decisions that optimize performance for the needs of the services, even if those decisions have a negative impact on NC3 capabilities. To remedy this imbalance, U.S. Strategic Command's role in making NC3 acquisition decisions, and indeed any decisions that relate to acquisition of dual-capable weapons systems and platforms, should be strengthened, preferably by giving that command the ability to allocate funding that supports its nuclear mission rather than only to oppose funding decisions that impede that mission.

Finally, entanglement of conventional and nuclear systems means that attacks on the former could affect — or be perceived to be intended to affect — the latter. And attacks, real or perceived, on a nation's nuclear systems are particularly escalatory if the nature of the conflict up to that point has been confined to the conventional domain. This unavoidable fact of life drives the imperative that nuclear-armed nations should do what they can to minimize the possibility that attacks on conventional assets will be seen as attacks on nuclear assets.

The third observation is that short timelines for decision-making increase cyber risk. In combat situations, commanders face the time pressure of deciding on a course of action, generally in the face of incomplete information. But when the stakes are high, waiting for more information may be the wisest course of action. For example, waiting may

[35] *National Security Strategy of the United States of America*, The White House, December 2017, 30, emphasis added, http://nssarchive.us/wp-content/uploads/2020/04/2017.pdf.

allow additional information to arrive showing that a signal indicating an incoming attack is in fact erroneous. Cyber risks arise from the possibility of hacker-induced malfunctions, which may delay the arrival of information or accidentally corrupt information flowing in the NC3 system, and from adversary hackers who may deliberately introduce misinformation into the system. Additional time can help to mitigate (though not eliminate) cyber risk by allowing system operators to confirm that information being provided by the NC3 system was not being corrupted or distorted as the result of adversary cyber activities.

The fourth observation is that the legacy NC3 system has not failed catastrophically. Thus, corrective procedures and technology have been deployed to fix problems that have arisen over the course of decades. No modernized system can possibly have such a track record of problems that have been fixed, because it takes 3 decades to develop 30 years of operational experience. The corresponding imperative is that a modernized system should do what the legacy system would do when faced with the same operational scenarios. As the legacy system morphs over time into the modernized system, legacy and modernized components should operate in parallel for an extended period of time, with the outputs of the modernized system checked against those of the legacy system. Admittedly, this practice would entail substantial additional costs and operational difficulties, but the consequences of catastrophic NC3 failure are so serious that mitigating them should be worth the cost.

The fifth observation is that the tension between keeping up with a rapidly changing environment and maintaining an adequate cyber security posture cannot be resolved — only managed. Efforts to enhance cyber security generally slow down schedules and delivery timelines and increase cost. Experience with commercial software development indicates that security considerations often — even usually — play second fiddle to delivery schedules.[36] There is no reason to expect that such pressures do not apply to military systems as well.

Accordingly, users, including those at the most senior levels with the authority to specify the requirements for functionality related to nuclear weapons and operations, and system architects and designers should be prepared to make tradeoffs between measures to reduce cyber risk and performance requirements. Sacrifices needed to mitigate cyber risk may come in different forms, including lengthier acquisition schedules, reduced functionality, higher cost, or cumbersome non-technological approaches. And since users are rarely willing to give up functionality for better cyber security, overseers of the nuclear acquisition process (i.e., civilians in the Department of Defense and Congress) will have to ensure that they approach these tradeoffs honestly.

The final observation is that the cyber security posture across the U.S. nuclear enterprise is highly heterogeneous, with some elements having weaker cyber security than others. Cyber vulnerabilities in the nuclear enterprise are almost certainly highly varied across its components, among the individual entities within each component, and indeed even across different operational scenarios, with some being more cyber-vulnerable than others. The imperative associated with this observation is that because operators generally do not know how secure their systems are, *all* operators should be taking the precautions that would be necessary if they were operating on systems and networks known to be compromised by an adversary. These operating practices will be inconvenient, reduce productivity, and seem unnecessary, but employing them is the only way to limit the effects of a security compromise.

In addition, as more operational functions of the nuclear enterprise become more automated, it will be important for humans to maintain the ability to perform at least a minimal set of these functions. This has two major advantages. First, it will give humans the ability to perform some degree of independent sanity checks on the computer-generated output they will be seeing. Second, and perhaps more importantly, human operators may well have to step into the breach if these automated functions are compromised for any reason. As an example, humans need to retain the ability to plan in-flight refueling for bombers, even as such planning is made more efficient through the use of computerized databases. Imposing a requirement that humans be able to take over a minimal set of functions will require engineering the system in ways that actually provide for the possibility of manual control. While obvious, such

[36] Seymour E. Goodman and Herbert S. Lin, eds., *Toward a Safer and More Secure Cyberspace*, National Research Council and National Academy of Engineering of the National Academies, , 2007, 66, https://doi.org/10.17226/11925; and David Clark, Thomas Berson, and Herbert Lin, eds., *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, National Research Council of the National Academies, 2014, 62 and 99, https://doi.org/10.17226/18749.

engineering has not always been performed in both civilian and military systems.[37]

Moving Forward

As the Biden administration's nuclear policy takes shape, it is hard to imagine developments that would challenge the overarching premise of this document — that issues of cyber security are critical to the whole of the nuclear enterprise. These issues pertain most strongly to the NC3 system, but many of the cyber security issues facing NC3 modernization also apply, in some form, to other aspects of the nuclear modernization program.

To reduce cyber risks to the nuclear enterprise, it should go without saying that sustained, high-level attention to cyber security issues will be necessary. Senior leadership within the Department of Defense has struggled over the last couple of decades to increase the priority of cyber security issues across the entire U.S. military establishment. Congress has expressed particular concerns about cyber risks to the nuclear enterprise: The FY2018 National Defense Authorization Act required the secretary of defense to provide an annual assessment of the cyber resiliency of the nuclear command-and-control system. Perhaps reflecting concerns about the results of the first assessment, the FY2021 National Defense Authorization Act required the secretary of defense to submit to the U.S. Congress a comprehensive plan to address cyber security issues identified in that assessment, including a concept of operations to defend the NC3 system from cyber attacks and develop an oversight mechanism to ensure implementation.

On the other hand, high-level policy attention to a cyber security issue does not necessarily translate into improved cyber security practices on the ground, as the response to the Government Accountability Office report described above indicates. Indeed, every official involved with the weapons systems examined by that office would agree that cyber security was and is an important issue to take into account in the acquisition of the systems for which they were responsible. And yet, they were confident that their efforts were adequate, discounting the Government Accountability Office's findings. Indeed, experience suggests the high likelihood that at least some important databases will be contained in unprotected and unauthenticated Excel files on someone's computer at work. That computer is probably on a protected classified network somewhere, but may well be otherwise undefended, leaving the database spreadsheets open to alteration.

Accordingly, some methodology is needed to establish what is actually happening on the ground. Perhaps the best way to do this is to make frequent use of red-teaming, where the red team is permitted to conduct its activities as a sophisticated, well-resourced, and determined adversary would conduct them and the reports of such exercises are made broadly available to program overseers — and not just program managers, who have incentives to benignly neglect cyber security issues. (I myself observed an Army brigade combat exercise involving an opposing force that was supposed to be free to innovate tactics against the brigade in training as it saw fit. However, conversations with the opposing force's red team revealed that it was in fact highly constrained in the cyber dimension.[38]) Program overseers should take concerted action to promptly remediate any problems that are identified in these exercises.

The observations and principles described in this paper are not new. It is possible that managers of the modernization effort have already systematically taken them to heart and have made, and will continue to make, tradeoffs with regard to system functionality to enhance cyber security. If so, that is a better outcome than what could normally be expected. Indeed, the entire history of cyber security is one of cyber security reports being issued and ignored. Some may presume that once good and actionable information on cyber security vulnerabilities is made available, those responsible will act on it. The reality is, they don't.

Thus, historical experience with cyber security issues in system acquisition, both civilian and military, would suggest caution. Although decision-makers generally acknowledge the importance of cyber security in principle, they rarely make compromises on other system functionality to improve cyber security. Regardless, the Biden administration has an opportunity to address issues of cyber risk across the entire nuclear enterprise in ways that previous administrations have not. Taking note of these observations and principles will not guarantee that the nuclear modernization effort will be adequate to protect against the future cyber threat — but ignoring them will surely guarantee that it will not be.

[37] Nick Bilton, "Nest Thermostat Glitch Leaves Users in the Cold," *New York Times*, Jan. 13, 2016, https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html; and Gregory Slabodkin, "Software Glitches Leave Navy Smart Ship Dead in the Water," *Government Computing News*, July 13, 1998, https://gcn.com/articles/1998/07/13/software-glitches-leave-navy-smart-ship-dead-in-the-water.aspx.

[38] Herb Lin, "Army Combat Exercise in Hawaii Plays Down Cyber Threat," *Lawfare*, Feb. 6, 2016, https://www.lawfareblog.com/army-combat-exercise-hawaii-plays-down-cyber-threat.

Herbert Lin *is senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University. His research interests relate broadly to policy-related dimensions of cyber security and cyberspace, and he is particularly interested in the use of offensive operations in cyberspace as instruments of national policy and in the security dimensions of information warfare and influence operations on national security. In addition to his positions at Stanford University, he is Chief Scientist, Emeritus for the Computer Science and Telecommunications Board, National Research Council of the National Academies, where he served from 1990 through 2014 as study director of major projects on public policy and information technology. He is also a member of the Science and Security Board of the Bulletin of Atomic Scientists. In 2016, he served on President Barack Obama's Commission on Enhancing National Cybersecurity. Prior to his National Research Council service, he was a professional staff member and staff scientist for the House Armed Services Committee (1986–1990), where his portfolio included defense policy and arms control issues. He received his doctorate in physics from the Massachusetts Institute of Technology.*

The material in this article is derived from the book "Cyber Threats and Nuclear Weapons," copyright Stanford University Press, forthcoming October 2021.

Image: Christiaan Colen (https://flickr.com/photos/christiaancolen/21382575392/), CC BY-SA 2.0 (https://creativecommons.org/licenses/by-sa/2.0/)