National Security Decision-Making in the Age of Technology: Delivering Outcomes On Time and On Target

Gary P. Corn*

Introduction

As anyone who has ever been responsible for or involved in significant decision-making knows, a failure to make a decision is, in itself, a decision.[1] And as the late Peter F. Drucker noted decades ago when discussing effective decision-making, inaction is not a risk-free proposition: "One has to make a decision when a condition is likely to degenerate if nothing is done. The effective decision-maker compares effort and risk of action to risk of inaction."[2] There is no area where this basic truism has more resonance, and is potentially more consequential, than in the area of national security decision-making, where the cost of inaction can be at a premium. Poorly informed or precipitous decisions and actions carry their own risks and can often lead to suboptimal results. But so too can decision delay and paralysis in the face of gathering or ongoing threats. As

* Director of the Technology, Law & Security Program and Adjunct Professor of Cyber and National Security Law at *American University Washington College of Law*; a member of the editorial board of the *Georgetown* Journal of National Security Law and Policy, and the Founder and Principal of Jus Novus Consulting, LLC. A retired U.S. Army colonel, Professor Corn previously served as the Staff Judge Advocate to U.S. Cyber Command, as a Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff, the Operational Law Branch Chief in the Office of the Judge Advocate General of the Army, the Staff Judge Advocate to United States Army South, on detail as a Special Assistant United States Attorney with the United States Attorney's Office for the District of Columbia, and on deployment to the Republic of North Macedonia as part of the United Nations Preventive Deployment Force and as the Chief of International Law for Combined Forces Command, Afghanistan. I would like to thank Tech, Law & Security Program Fellow Justin Sherman for his assistance in putting this essay together.

[1] The familiar adage is attributed to the American philosopher and psychologist William James. *See* 2 William James, The Principles of Psychology 532-534 (Dover Publ'n 1950) (1890).

[2] Peter F. Drucker, Management: Tasks, Responsibilities, Practices 475-76 (1974).

the Romans learned long ago, fiddling in the face of a crisis can be both disastrous and a dereliction.

Finding the right balance between decision-making processes that facilitate timely, well-informed and coordinated national-security decisions and those that Nero would have admired has never been easy, with successive administrations and National Security Councils (NSCs) wrestling with this dilemma in different ways. While in theory most everyone will rail against overly bureaucratic processes and eschew the proverbial "long screwdriver," in practice it often becomes the tool of choice for managing, or better stated, avoiding risk.[3] But one thing has become very clear in the years since the tragic events of September 11th: advances in technology and the increasingly complex nature of the national security threats they engender have exacerbated, not alleviated, this dilemma. Emerging technology has introduced new and complex threats that, in many instances, compress decision space and timelines and magnify the risks of inaction.

When it comes to national security, new technologies have always been a double-edged sword of opportunity and risk. In the past, owing to its dominance in technology development, the United States was generally able to blunt, or at least forestall, the risk side of the blade while reaping the benefits of new technology. This was certainly the case in the initial years after September 11th, at least with respect to the counterterror and insurgency operations that until recently dominated the national security landscape.

But owing to myriad factors—not the least of which is the unprecedented shift of research, development, and dissemination of technology to the private sector —the United States can no longer rely on a distinct competitive edge over its adversaries, especially in light of the reemergence of near-peer, nation-state adversaries and the return of so-called Great Power Competition. Not only has the lag time between the development of new technologies and their general proliferation diminished significantly, in many instances, our adversaries threaten to beat us to market or outpace us. According to the most recent *Annual Threat Assessment of the U.S. Intelligence Community*, this trend will continue: "Following decades of investments and efforts by multiple countries that have increased their technological capability, US leadership in emerging technologies is increasingly challenged, primarily by China. We anticipate that with a more level playing field, new technological developments will increasingly emerge from multiple countries and with less warning."[4] The rapid evolution of cyberspace, the hyper-competitive state of relative cyber capabilities and capacity, and

[3] The "long screwdriver" is a well-known metaphorical reference to micromanagement from Washington of national security operations, first coined by Admiral Joseph Metcalf during the Vietnam War. *See*, Christopher J Lamb, *The Micromanagement Myth and Mission Command: Making the Case for Oversight of Military Operations*, 33 INST. NAT'L STRAT. STUDIES STRAT. PERSPECTIVES 1, 11 n. 49 (2020)(citations omitted), https://perma.cc/TE4F-W2DA.

[4] OFF. DIR. NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 20 (2021).

the prolific use of cyber operations in the strategic, quasi-conflict space of the so-called "gray zone" is a prime example.

Although the cyber threat landscape is still nascent and evolving, it is painfully clear that as a nation we have been shooting behind the target for too long. As recent events like the Solar Winds Breach, the Microsoft Exchange Server hack, and the ransomware operation against Colonial Pipeline all demonstrate, we have yet to achieve an acceptable level of national cyber security. While this overall cyber insecurity is not the result of any single cause or failure, important lessons have emerged about the costs of decision delay and inaction that should be instructive for how we approach other emerging technologies. The well-documented shift in 2018 to a more proactive cyber strategy was premised in large measure on the recognition that the prior policy of restraint and concomitant failure to respond to cyber threats in a timely and meaningful way had encouraged, not deterred, our adversaries.[5] Implementation of this new strategy therefore required the adoption of a more responsive decision-making process for approving cyber operations; one that was better aligned to the hyper-dynamic and time-sensitive nature of the threat. Moving forward, the national-security decision-making apparatus must account for the increasingly compressed decision space characteristic of emerging technologies.

I. DECISIONS DELAYED ARE DECISIONS DENIED

The same dynamics that drove replacement of the Obama-era policy with *National Security Presidential Memorandum (NSPM) 13, United States Cyber Operations Policy*, are also implicated by a host of emerging technologies, from Artificial Intelligence (AI), to drones and drone swarms, to space capabilities, and more.[6] Although each presents different risk considerations, one thread is common to most emerging-technology threats—decision timelines are growing increasingly compressed, and a decision delayed is a decision denied. National security decision-making processes must account for this growing reality.

A. The Promise and Threat of Emerging Technology and the Shrinking OODA Loop

Emerging technologies "pose[] both peril and promise."[7] Technology is reshaping the world at an exceptional pace and scale, especially with regard to how individuals, institutions, and nations all interact. The current and future benefits of technology are substantial and often obvious. Digital interconnection, the democratization of knowledge, and the record-setting speed of the development

[5] Under the Obama administration, it was stated policy "that we shall undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as preferred courses of action." OFF. OF THE WHITE HOUSE PRESS SEC'Y, FACT SHEET ON PRESIDENTIAL POLICY DIRECTIVE 20 (2013).

[6] Honorable Paul C. Ney, Jr., Gen. Couns., Dep't of Def., Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020) https://perma.cc/3357-TZHG.

[7] WHITE HOUSE, INTERIM NATIONAL SECURITY STRATEGIC GUIDANCE 7-8 (2021).

and deployment of COVID-19 vaccines are just a few examples. As long as the U.S. maintains a competitive advantage on defense and other national security related technologies, the benefit of those capabilities should be apparent.

At the same time, "the direction and consequences of the technological revolution remain unsettled," as emerging technologies "remain largely ungoverned by laws or norms designed to center rights and democratic values, foster cooperation, establish guardrails against misuse or malign action, and reduce uncertainty and manage the risk that competition will lead to conflict."[8] State and non-state threat actors are leveraging technology at an increasing rate to erode U.S. power, influence and security. According to the Intelligence Community (IC):

> New technologies, rapidly diffusing around the world, put increasingly sophisticated capabilities in the hands of small groups and individuals as well as enhancing the capabilities of nation states. While democratization of technology can be beneficial, it can also be economically, militarily, and socially destabilizing. For this reason, advances in technologies such as computing, biotechnology, artificial intelligence, and manufacturing warrant extra attention to anticipate the trajectories of emerging technologies and understand their implications for security.[9]

Technology is rapidly diminishing the security of geography and distance, affording our adversaries options and advantages that they previously lacked. The ability to reach across the globe in near-real-time to steal or manipulate critical information, influence populations, interfere in democratic processes and governance, and damage critical infrastructure, are just a few examples. Technology enables threat actors to challenge U.S. national security in novel ways and with unprecedented scope, scale, depth, and critically, speed. Although (as of the time of this writing) attribution of the Colonial Pipeline shutdown remains uncertain, the reach and speed with which a threat actor was able to disrupt fuel distribution across the eastern United States has profound national security implications.[10]

Clearly, if properly managed, technology can and should be used to enhance national security decision-making and actions. However, technology can both stress and compress the decision-making cycle. Consider technology's impact within the frame of Colonel John Boyd's now famous Observe, Orient, Decide, Act—or OODA—Loop decision framework, which he developed to outpace his enemy's decisions in the chaotic and face-paced environment of air-to-air combat.[11] On the one hand, the ability to collect, process, and disseminate data and information—the key to observing and orienting—is now nearly unbounded and will only increase with improvements in big-data analytics, AI, and Quantum

[8] *Id.* at 8-9.

[9] OFF. DIR. NAT'L INTEL., *supra* note 4.

[10] David E. Sanger & Nicole Perlroth, *Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity*, N.Y. TIMES (May 14, 2021), https://perma.cc/HUW3-VA4P.

[11] JOHN R. BOYD, A DISCOURSE ON WINNING AND LOSING (2018), https://perma.cc/8XR9-R7EA.

computing. At first blush, this should be viewed as a net positive. But like Say's law of economics, the unending supply of information creates its own demand which can become insatiable for a decision-maker, and lead quickly to information overload and decision paralysis.[12] Decisions made on imperfect or incomplete information carry inherent risk, and the knowledge that there is potentially more to gather is often the safe space of the risk averse. Also, the real-time command and control reach that technology enables is tempting fare for the risk averse and those inclined to wield the long screwdriver.

Conversely, as then Chairman of the Joint Chiefs of Staff, General Joseph Dunford noted in 2018, "[a]dvancements in space, information systems, cyberspace, electronic warfare, and missile technology have accelerated the speed and complexity of war. As a result, decision space has collapsed. . . ."[13] General Dunford's observation is not limited to warfare, but extends across the entirety of the national security landscape. The technology-enabled threats posed to U.S. national security today—from adversaries, from nonstate threat actors, and even from the risk that critical technological systems fail—compel a compressed decision-to-action timeline that can respond to and outpace threats in real-time.

This collapsing decision space naturally involves risk, the tolerance of which must be balanced against the consequences of delay or inaction. For example, unmanned combat systems, such as drone swarms and other artificial intelligence-powered weaponry, act rapidly and thus necessitate the use of automated defensive systems that can respond to and mitigate those threats on a proportionately compressed timeline. This is because the speed of human decision-making, as Army Futures Command head General John Murray has stated, is likely insufficient for fighting automated kinetic threats like swarms of enemy drones, leaving automated decision-making as a potentially more, and perhaps the only, viable option.[14] Managing each of these engagement decisions out of the White House is simply infeasible.

Another example of the need for greater speed and agility in national security decision-making is the specter of autonomous or self-adapting cyber threats. The Defense Advanced Research Projects Agency (DARPA) has already demonstrated that self-learning worms that can scan, patch vulnerabilities, and potentially exploit networks and systems on the fly are not theoretical.[15] Such capabilities could be deployed in the not-too-distant future both against the United States and as a tool to counter cyber threats. For instance, one DARPA project is focused on developing autonomous software to "counter malicious

[12] *Say's law: supply creates its own demand*, ECONOMIST (Aug. 12, 2017), https://perma.cc/JXM9-Z372.

[13] General Joseph F. Dunford, Jr., *The Character of War and Strategic Landscape Have Changed*, 89 JOINT FORCE Q. 2, 2 (2018), https://perma.cc/KL85-KHQ8.

[14] *See* David Hambling, *Drone Swarms Are Getting Too Fast for Humans to Fight, U.S. General Warns*, FORBES (Jan. 27, 2021, 10:43 AM), https://perma.cc/PH5W-54ZU.

[15] Patrick Tucker, *Trump's Pick for NSA/CyberCom Chief Wants to Enlist AI for Cyber Offense*, DEF. ONE (Jan. 9, 2018), https://perma.cc/XT2U-9GZK.

botnet implants and similar large-scale malware."[16] If cyber threats have accelerated the speed and complexity of conflict, the OODA Loop timelines of these automated cyber engagements will be measured in nanoseconds, not the months to years that marked deliberations over cyber operations in the past—at least until 2018.

B. NSPM-13, U.S. Cyber Operations, and the "Speed of Relevance"

The year 2018 saw a sea change in the U.S. government's approach to cyber threats. Changes in strategy, legislation, and policy all served to reorient the U.S. from a posture of restraint and relative inaction, to one of proaction and persistent engagement in cyberspace.[17] This shift was in no small measure driven by the leadership of then Secretary of Defense James Mattis and General Dunford, who recognized the changing face of national security threats and the need to fundamentally change the decision-making culture within the Department of Defense and the broader national security community.[18] They are both credited with coining a phrase that is now *de rigueur* in DoD lexicon: *the speed of relevance*—the notion that decisions and actions must be relevant to and outpace our threats.[19] Leaving aside the obvious question of just how one measures how fast relevance moves, their insight and objective in using this rhetorical tool deserves praise. Both recognized that outmoded and overly bureaucratic processes as well as a culture of risk aversion were maladapted to the current threat environment and needed to change.

Also issued in 2018, NSPM-13 was aimed precisely at adapting the national security decision-making cycle to the realities of cyberspace. It replaced Presidential Policy Directive (PPD)-20, issued under the Obama administration, which previously established the U.S. government review process for cyber operations—a process that was notorious for reinforcing indecision.[20] According to Brigadier General Alexus Grynkewich, then serving as the Deputy Director for Global Operations on the Joint Staff, PPD-20 required "an interagency process that went through the National Security Council and all the way up from a policy coordination committee to a deputies' committee to a principals' committee," effectively meaning "anyone could stop the process at any point."[21] In contrast, NSPM-13 provides "for the delegation of well-defined authorities to the

[16] DUSTIN FRAZE, DEF. ADVANCED RSCH. PROJECTS AGENCY, HARNESSING AUTONOMY FOR COUNTERING CYBERADVERSARY SYSTEMS (HACCS), https://perma.cc/KFW4-DLF6.

[17] *See* Gary P. Corn & Emily Goldman, *Defend Forward and Persistent Engagement*, *in* THE UNITED STATES' CYBER STRATEGY AND "DEFEND FORWARD": A COMPREHENSIVE LEGAL ASSESSMENT (forthcoming 2022).

[18] *See* Joe Dransfield, *How Relevant is the Speed of Relevance?: Unity of Effort Towards Decision Superiority is Critical to Future U.S. Military Dominance*, STRATEGY BRIDGE (Jan. 13, 2020), https://perma.cc/26DE-F5MN.

[19] *Id.*

[20] *See* Robert Chesney, *CYBERCOM's Out-of-Network Operations: What Has and Has Not Changed Over the Past Year?*, LAWFARE (May 9, 2019, 5:56 PM), https://perma.cc/4NUB-2UQ6.

[21] Sydney J. Freedberg, Jr., *Trump Eases Cyber Ops, But Safeguards Remain: Joint Staff*, BREAKING DEF. (Sept. 17, 2018, 5:30 PM), https://perma.cc/WKJ3-3XJ5.

Secretary of Defense to conduct time-sensitive military operations in cyberspace."[22] In line with the shift to a more proactive cyber strategy noted above, NSPM-13 enables faster, more agile decision-making better adapted to the strategic threat. It does so not only by allowing delegations of authority, but by reinforcing those delegations with a coordination and approval process run by the delegee, not the NSC.[23]

Because NSPM-13 remains classified, it is difficult to fully gauge whether it strikes the right balance between speed and sufficiently coordinated decisions, but indications thus far are that it has achieved the objective of enabling more agile responses to cyber threats. Starting with the widely reported and successful operations in defense of the 2018 mid-term elections, General Nakasone, the Commander of U.S. Cyber Command, has steadily implemented his approach of persistent engagement and defend forward operations and activities, acknowledging that the command has conducted dozens of operations to counter foreign cyber and influence threats.[24] Obviously there is no one-size-fits-all model for posturing the national security apparatus to manage each distinct threat scenario, but there are important lessons to be taken from the NSPM-13 effort to adopt "a more agile, expeditious decision-making structure."[25]

II. PROCESS SHOULD ENABLE OUTCOMES, NOT PROCESS (AKA FIGHT THE THREAT, NOT EACH OTHER)

Replacing PPD-20 was no small task. For some time, the process was bogged down by "bureaucratic inertia, turf fights, and some genuine unresolved issues . . . ."[26] As Brigadier General Grynkewich noted, whether intended or not, PPD-20 afforded departments and agencies a means to deadlock the approval process, and thereby in effect, make decisions through inaction.[27] The motives behind any such instance are knowable only to those involved and could at times have been based on "genuine unresolved" legal, policy, or risk concerns, but the "turf wars" that National Security Advisor Bolton alluded to cannot, in all circumstances, be ruled out.[28] Either way, an effective decision-making process should be designed to aid the designated decision-maker in rendering a decision. A process that allows participants to effectively usurp decision authority without the attendant accountability is a design flaw, not a feature.

Imposing process for process' sake is a fool's errand, unless the objective is to drive interminable debate and bureaucratic inertia. Process is a means to an end, not an end in itself, and so it should always be designed to fulfill an objective. In

[22] Ney, *supra* note 6.

[23] *See* Freedberg, *supra* note 21.

[24] *See* Press Release, Joint Chiefs of Staff, Cyber Command Expects Lessons from 2018 Midterms to Apply in 2020, https://perma.cc/6FVE-UB3Z.

[25] Shannon Vavra, *Here's What John Bolton had to Say About Cybersecurity Policy in his New Book*, CYBERSCOOP (June 22, 2020), https://perma.cc/ST4E-Q8KF.

[26] *Id.*

[27] Freedburg, *supra* note 21.

[28] *See* Vavra, *supra* note 25.

the case of national security decision-making, the objective is to achieve the most well-informed decision possible under a given set of circumstances, including acceptable risk parameters and time available. The increasingly complex, fast-moving, and dynamic nature of modern national security threats requires disciplined decentralization of action consistent with centralized intent. This generally starts with delegating decision authority to the official best-suited to make—and who will be held accountable for—the decision. The process should then be designed to assist that decisionmaker by identifying and presenting the information relevant to making the decision, as well as involving the departments, agencies or other stakeholders who can provide that information or have a key stake in the decision to be taken.

Unfortunately, the same players who should be facilitating decisions often leverage aspects of existing processes to push parochial, institutional agendas. Some have described the interagency process generally as a forum for fighting ourselves far harder than we fight our adversaries.[29] When process is allowed to disfunction in this way, it fails. This is not to say that there are not legitimate legal and policy questions that need to be vetted as part of an informed decision-making process; the law of unintended consequences among them. But often, rather than serving as a forcing function to resolve these issues, they are raised as a proxy for interagency disputes and power struggles.

Consider an issue that plagued the cyber-operations approval process for years —the applicability of the Covert Action Statute (CAS) to DoD cyber operations.[30] On its face, the CAS is more of a procedural than a substantive statute and leaves to the President's discretion the decision as to which department or agency will conduct a particular covert action.[31] However, as a matter of longstanding policy, the conduct of covert action is the sole province of the Central Intelligence Agency,[32] and the CAS is often invoked within the interagency as substantively demarcating the boundaries of institutional roles and authorities. As a result, unless a proposed activity falls within one of the enumerated and narrowly construed exceptions to the CAS's definition of covert action—such as the exception for traditional military activities (TMAs) in the case of DoD operations— the CAS is frequently invoked as a bar to action. Given the inherently clandestine nature of cyber operations, the CAS proved to be a substantial obstacle in the approval process for DoD operations until Congress stepped in with the passage of Section 1632 of the National Defense Authorization Act (NDAA) for fiscal year 2019, which defined clandestine military cyber operations as TMAs.[33] In doing so, Congress noted

[29] *Id.*; *see also* John Hamre, *Reflections: Improving the Interagency Process*, DEF.360 (Feb. 23, 2016), https://perma.cc/48FU-Z8V9.

[30] 50 U.S.C. § 3093.

[31] 5 U.S.C. § 3093(a).

[32] *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *as amended by* Exec. Order No. 13,470 § 1.7 (a), U.S. Intelligence Activities 73 Fed. Reg. 45325 (July 30, 2008); *see also* 50 U.S.C. § 3093(a)(3).

[33] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232 (Aug. 13, 2018) § 1632.

its displeasure that the perceived ambiguity as to whether DoD cyber operations qualified as TMA had been the cause of "difficulties within the interagency in obtaining mission approval," with the "unfortunate [result] that the executive branch [had] squandered years in interagency deliberations. . . ."[34]

The point is not to litigate the merits of the CAS versus TMA debate. It is to highlight that institutional parochialism and interests are a reality of the interagency structure that have to be guarded against, not incentivized or facilitated. Legitimate legal and policy issues (and ambiguities) are part of the risk calculus that must be considered in any decision-making process. They should not be leveraged as proxies for institutional jockeying, however, as the responsibility for reaching a decision ultimately lies with one official, and not with the process itself. Given the increasingly compressed decision-making cycle that new technologies and national-security threats require, we can ill afford processes that impede, delay, or effectively usurp decision-making authority. This holds true no matter which department or agency will be delegated decision authority or tasked to act.[35]

III. MOVING FORWARD

In the high-stakes arena of national security, decision-making is ultimately about risk management and the singular focus of any decision-making process should be to drive sound, risk-informed, but timely decisions. In the face of a given national security threat, inaction may prove to be the best course to follow. But like any potential course of action, the decision not to act must be a deliberate one, taken after comparing the risks and rewards of inaction over action. On the other hand, inaction born of decision delay or paralysis, or even worse, decision avoidance, is an unacceptable outcome bordering on dereliction. Unfortunately, emerging technologies will likely continue to make this calculus harder as decision space and timelines condense and the imminence of threats increases. National security decision-making processes must account for this factor moving forward.

The replacement of PPD-20 with NSPM-13 serves as an example of how the dynamics of national security decision-making are changing, necessitating more agile and responsive approval processes for confronting emerging threats. PPD-20 was apparently designed to provide oversight, coordination, and interagency review of cyber operations, but it proved too slow and cumbersome, withheld risk decisions at unrealistic levels, and allowed interagency coordination to stifle decisions. Risk, policy and legal considerations, and interagency equities remain important and should be accounted for in any decision-making process, but not in a

[34] H.R. REP. NO. 115-874, at 1049 (2018) (Conf. Rep.).

[35] *See* Zach Dorfman, Kim Zetter, Jenna McLaughlin & Sean D. Naylor, *Exclusive: Secret Trump order gives CIA more powers to launch cyberattacks,* YAHOO! NEWS (July 15, 2020), https://perma.cc/J2A7-UJZG; Robert Chesney, *The CIA, Covert Action and Operations in Cyberspace*, LAWFARE BLOG (July 15, 2020, 3:43 PM), https://perma.cc/V7JP-GDVS (noting for example, reports of the President delegating greater flexibility for cyber covert action to the CIA in 2018).

way that allows process to usurp decision authority and accountability. As we face new threats and new areas of technology that we will need to protect against and employ in our national interest, we should build on the lessons we have learned in the context of cyber operations and ensure decision-making processes account for the increasingly compressed decision space and timeliness that leaders will face.