William & Mary Bill of Rights Journal

Volume *26 (2017-2018)*
Issue 2 *Symposium: Big Data, National Security, and the Fourth Amendment*
Article 5

December 2017

Encryption, Asymmetric Warfare, and the Need for Lawful Access

Geoffrey S. Corn

ENCRYPTION, ASYMMETRIC WARFARE, AND THE NEED FOR LAWFUL ACCESS

Geoffrey S. Corn*

More than three decades ago, I reported for my training as a U.S. Army military intelligence officer. I really had no idea what to expect. Having enlisted in the Army six months earlier and successfully completed Initial Entry Training and Officer Candidate School, I knew very little about the focus of the training I was about to begin. "Intelligence" brought to my mind clandestine activities; but I would soon learn that such activities were a relatively insignificant focus of my training. Instead, I would learn everything possible about the enemy our nation considered its most likely and dangerous threat at that time—the Soviet military.

I quickly learned that "intelligence" is the essential predicate to the efficient and effective use of combat power to achieve tactical, operational, and strategic objectives.[1] My function as a staff intelligence officer would be to contribute to the mission planning and execution process by providing that predicate. But the broader lesson I learned then, and during my several years performing that function for Army units in Panama, was that knowing how the enemy operates is what enables exploitation of enemy vulnerabilities and protection against enemy capabilities.

The world has obviously changed substantially since 1984 (although the prospect of a "new" Cold War with Russia is an increasingly significant national security concern).[2] Transnational terrorism is now considered a primary national security

* Professor of Law and Presidential Research Professor, South Texas College of Law Houston; Lieutenant Colonel (Retired), U.S. Army Judge Advocate General's Corps. Prior to joining the faculty at South Texas, Professor Corn served in a variety of military assignments, including as the Army's Senior Law of War Advisor, Supervisory Defense Counsel for the Western United States, Chief of International Law for U.S. Army Europe, and as a Tactical Intelligence Officer in Panama.

[1] *See generally* U.S. DEP'T OF THE ARMY, ARMY DOCTRINE REFERENCE PUBLICATION 2-0, INTELLIGENCE (2012).

[2] *See* Evan Osnos et al., *Trump, Putin, and the New Cold War: What Lay Behind Russia's Interference in the 2016 Election—And What Lies Ahead?*, NEW YORKER (Mar. 6, 2017),

threat.[3] In ways too numerous to catalogue in this Article, that threat is substantially different than the former prospect of a full-scale war with the Soviet Union.[4] Nonetheless, in response to transnational terrorism, the basic function of intelligence is really no different than it was in response to the Soviet threat: identify enemy strengths and weaknesses, predict enemy course of action, and maximize the effectiveness of our response by ensuring it is directed towards the right objectives.

But the differences in this threat certainly make the process of gathering vital intelligence different. Unlike the conventional military threat represented by the Soviet Union, transnational terrorist groups are remarkably adept at operating in the shadows and cloaking intentions, capabilities, and vulnerabilities to frustrate U.S. counterterrorism efforts.[5] Indeed, the very nature of this struggle is defined by asymmetry—asymmetry in the capabilities of the foes, asymmetry in the nature of the targets each seeks to strike, asymmetry in respect for the rule of law in relation to operations, and asymmetry in the very definition of success.[6] These asymmetries inevitably impact the means and methods of effective counterterrorism operations.

For the transnational terrorist enemy, rule of law is an anathema.[7] Indeed, law is a tool they seek to exploit to gain tactical and strategic advantage.[8] These enemies know law will inevitably impose constraints on their more advanced opponents, and that these constraints provide maneuver space that can be exploited to achieve their objectives. In contrast, the United States views law not as a constraint, but as an essential foundation for ensuring the legitimacy of our counterterrorism operations.[9]

---

https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war [https://perma.cc/JB3S-TNTX]. *But see* Michael Cohen, *Peace in the Post–Cold War World: The World Is a Much Safer Place Than It Was 20 Years Ago—Here's Why, How It Happened, and What It Means for Our Future*, ATLANTIC (Dec. 15, 2011), https://www.theatlantic.com/international/archive/2011/12/peace-in-the-post-cold-war-world/249863 [https://perma.cc/C3UL-6DEG].

[3] THE WHITE HOUSE, NATIONAL STRATEGY FOR COMBATING TERRORISM 1 (2006).

[4] *Compare* NAT'L SEC. COUNCIL, NSC 68: UNITED STATES OBJECTIVES AND PROGRAMS FOR NATIONAL SECURITY (1950), *with* DANIEL R. COATS, WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY (2017) (statement from the Director of National Intelligence to the Senate Select Committee on Intelligence).

[5] THE WHITE HOUSE, NATIONAL STRATEGY FOR COMBATING TERRORISM 7–8 (2003).

[6] *See generally* Ayaz Ahmed Kahn, *Terrorism and Asymmetrical Warfare: International and Regional Implications*, DEFENCE J. (Pak.), http://www.defencejournal.com/2002/february/terrorism.htm [https://perma.cc/L8M9-6EUQ] (last visited Dec. 4, 2017); *Asymmetric Warfare*, RAND CORP., http://www.rand.org/topics/asymmetric-warfare.html [https://perma.cc/UG3R-5ZSH] (last visited Dec. 4, 2017).

[7] *See, e.g.*, *How Do You Define Terrorism?*, ABC NEWS (Oct. 11, 2001), http://abcnews.go.com/US/story?id=92340 [https://perma.cc/G88S-2FJJ].

[8] *See generally, e.g.*, Emanuel Gross, *Use of Civilians as Human Shields: What Legal and Moral Restrictions Pertain to a War Waged by a Democratic State Against Terrorism?*, 16 EMORY INT'L L. REV. 445 (2002).

[9] THE WHITE HOUSE, NATIONAL SECURITY STRATEGY 19–20 (2015), http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf [https://perma.cc/B4KF-Y3LA]; JOINT CHIEFS OF

While U.S. legal interpretations may not always be viewed as ideal or valid by domestic and international audiences, no one can seriously question U.S. commitment to acting within established legal frameworks when executing national security policies.[10] Nonetheless, the inevitable limitations on national power that result from these legal frameworks can at times be exploited by the terrorist enemy.[11]

The risks associated with the threat of transnational terrorism and the measures employed to deter, disrupt, and possibly defeat such threats are also complicated by the undeniable fact that this "enemy" straddles the line between law enforcement and armed conflict. Indeed, one of the most complex aspects of the U.S. response to transnational terrorism has been identifying if and when the use of military power is justified pursuant to the law of armed conflict.[12] Unlike past conflicts, however, criminal law tools are not a minor complement to war powers.[13] Instead, in this ongoing struggle, both criminal law and military powers are used extensively to achieve national security objectives.[14]

The invocation of war powers has not, however, been uncontroversial. Both international lawyers and civil libertarians have frequently criticized what they assert is the overzealous use of war powers in response to this threat.[15] In this sense, this "conflict" is truly unique, as it involves a threat that often may be effectively addressed through the use of criminal law powers instead of war powers. Indeed, one truly

---

STAFF, JOINT PUBLICATION 3-0, JOINT OPERATIONS I-5 (2017), http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf [https://perma.cc/M3QX-9YA5] ("National strategic direction is governed by the Constitution, federal law, USG policy, internationally recognized law, and the national interest as represented by national security policy.").

[10] *See* Geoffrey S. Corn & Tanweer Kaleemullah, *The Military Response to Criminal Violent Extremist Groups: Aligning Use of Force Presumptions with Threat Reality*, 47 ISR. L. REV. 253, 281–83 (2014).

[11] *See Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy: Hearing Before the S. Judiciary Comm.*, 114th Cong. (2015) (statement of James Comey, Director, Federal Bureau of Investigation, and Sally Quillian Yates, Deputy Attorney General); David P. Fidler, *Despite Progress, Combating Terrorist Exploitation of Cyberspace Faces Mounting Problems*, COUNCIL ON FOREIGN REL. (Aug. 2, 2017), https://cfr.org/blog/despite-progress-combating-terrorist-exploitation-cyberspace-faces-mounting-problems [https://perma.cc/K6YM-FF8A].

[12] *See* KENNETH WATKIN, FIGHTING AT THE LEGAL BOUNDARIES: CONTROLLING THE USE OF FORCE IN CONTEMPORARY CONFLICT (2016); *see also* THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 5–7 (2002); George Terwilliger et al., *The War on Terrorism: Law Enforcement or National Security?*, FEDERALIST SOC'Y (Feb. 15, 2005), http://www.fedsoc.org/publications/detail/the-war-on-terrorism-law-enforcement-or-national-security [https://perma.cc/T8NG-QLHS].

[13] *See* David Glazier, *Playing by the Rules: Combating Al Qaeda Within the Law of War*, 51 WM. & MARY L. REV. 957, 967–72 (2009).

[14] *See id.*

[15] *See, e.g.*, Mary Ellen O'Connell, *The Choice of Law Against Terrorism*, 4 J. NAT'L SEC. L. & POL'Y 343, 368 (2010).

unique aspect of the response to transnational terrorism is that military power may be more of a complement to criminal law powers.

But while this may be unique in the history of American wars, it is arguably illustrative of an emerging "threat response" paradigm—one in which peacetime legal response mechanisms are viewed as the norm, with periodic necessity *and* legal justification to expand national response authorities to those provided by military force operating pursuant to the law of armed conflict. As one distinguished author explains, this may be the true nature of "fighting at the legal boundaries."[16]

There are inherent dangers in this paradigm, both to security and liberty. From a security perspective, viewing the tools of armed conflict as the exception rather than the norm may offer terrorist enemies opportunities that might not otherwise exist. In this sense, the government and the people must assume a certain degree of additional risk that could be averted by treating every aspect of transnational terrorism as a wartime issue. However, from a liberty perspective, a wartime approach poses a substantial risk that government power will be exercised in a manner inconsistent with our core values. This is no exaggerated risk. The motivation of our very own national experiment came in part from revulsion to the overzealous use of military power by the Crown and the erosion of individual liberties it produced.[17] That revulsion made its way into the Constitution, the Bill of Rights, and, following the experience of Reconstruction after the Civil War, into federal legislation that strictly limited the permissible use of federal military forces to respond to domestic threats.[18]

Surveillance is one area where the balance between wartime and peacetime threat response authority is particularly important. For example, consider a display from a recent congressional hearing. In this example, the Director of the Federal Bureau of Investigation (FBI) and the Admiral commanding the National Security Agency (NSA) appeared together in a congressional hearing focused on surveillance of the Trump campaign and Russian efforts to influence the 2016 national election.[19] The mere visual impression left by this provides a reminder of the growing intersection of civilian and military intelligence and surveillance capabilities. Furthermore, the nature of cyber threats has also blurred the line between wartime and peacetime powers, a blurring that is exacerbated by the difficulty of even characterizing the

---

[16] *See* WATKIN, *supra* note 12, at 3–30.

[17] *American Revolution History*, HISTORY (2009), https://www.history.com/topics/american-revolution/american-revolution-history [https://perma.cc/PX9N-NTZE].

[18] *See* Posse Comitatus Act, 18 U.S.C. § 1385 (2012); *see also* GEOFFREY CORN ET AL., NATIONAL SECURITY LAW: PRINCIPLES AND POLICY 462–65 (2015) (providing a more nuanced discussion of the Posse Comitatus Act and the general prohibition on the use of federal military intervention in domestic affairs).

[19] *See Excerpts from the House Intelligence Committee Hearing on Russia*, N.Y. TIMES (Mar. 20, 2017), https://www.nytimes.com/2017/03/20/us/politics/james-comey-mike-rogers-transcript-excerpts.html?_r=0.

very nature of cyber operations.[20] Because "cyber" involves aspects of traditional criminal threats, espionage, and wartime threats,[21] it may be logical that U.S. cyber "operations" involve close coordination between civilian and military authorities. But this also indicates how tempting it will be in the future to characterize issues as wartime in nature, in order to maximize the military role in response measures.

All of these considerations point to a common imperative—ensuring that peacetime law enforcement response capabilities are not significantly hobbled by the intersection of emerging privacy, technology, and restrictive Fourth Amendment interpretations. As I have argued in other publications, I believe the Fourth Amendment actually supports government policies that ensure lawful access to "dark" spaces.[22] Accordingly, I have proposed the imposition of a "split key" creation and retention obligation imposed on entities that market end-to-end encryption (E2EE) for personal electronic devices such as smart phones.[23] While I recognize that such a requirement will increase the risk of unauthorized government access to private data, and possibly the risk of private security breaches, that risk is inherent in almost all other zones of individual privacy.

In this Article, I argue that the interest in ensuring a fair balance between privacy and government access to data is supported by another consideration, one that I have hinted to above—the risk of incentivizing the expansion of wartime-based authorities to access such data. To this end, I will first summarize my previously asserted Fourth

---

[20] "Encryption" is the process of encoding data so that only those with authorized access can read it. James Titcomb, *What Is Encryption, How Does It Work and What Apps Use It?*, TELEGRAPH (U.K.) (Mar. 29, 2017, 11:37 AM), http://www.telegraph.co.uk/technology/0/encryption-should-using/ [https://perma.cc/TVY7-6AMX]. A basic tenet of cryptography is that the security of the cryptosystem should rely upon the secrecy of the key and not the secrecy of the system's encryption algorithm. SUSAN LANDAU, SURVEILLANCE OR SECURITY?: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 43 (2010). Unlike earlier forms of encryption provided by telecommunications companies, *see generally* Andrew W. Yung, *Regulating the Genie: Effective Wiretaps in the Information Age*, 101 DICK. L. REV. 95 (1996), modern encryption methods are solely controlled by the user, *see* J. Riley Atwood, Comment, *The Encryption Problem: Why the Courts and Technology Are Creating a Mess for Law Enforcement*, 34 ST. LOUIS PUB. L. REV. 407, 407, 410–12 (2015). This has made it increasingly difficult for the government to obtain access to digital communications and information—even where pursuant to lawful authorization. *See generally* Jamil N. Jaffer & Daniel J. Rosenthal, *Decrypting Our Security: A Bipartisan Argument for a Rational Solution to the Encryption Challenge*, 24 CATH. U. J.L. & TECH. 273 (2016). This growing difficulty, and perhaps eventual impossibility, is often described as "going dark." Christopher Babiarz, *Encryption Friction*, 10 ALB. GOV'T L. REV. 351, 354 (2017).

[21] *See* Jessica R. Gross, Note, *Hack and Be Hacked: A Framework for the United States to Respond to Non-State Actors in Cyberspace*, 46 CAL. W. INT'L L.J. 109, 122–37 (2016).

[22] *See* Geoffrey S. Corn & Dru Brenner-Beck, *"Going Dark": Encryption, Privacy, Liberty, and Security in the "Golden Age of Surveillance," in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 330 (David Gray & Stephen E. Henderson eds., 2017).

[23] *Id.* at 361–62.

Amendment balance argument. I will then discuss the nature of transnational terrorist threats and how their reliance on asymmetric tactics creates an imperative for avoiding legal interpretations that provide the dark spaces they seek to exploit, especially in relation to communications. This will lead to a discussion of the increasingly "individualized" nature of armed conflicts against transnational terrorist enemies such as al Qaeda and ISIS, and how this individualization has and will continue to influence the perceived imperative of access to individual communications and data. The Article will then argue that the current boundaries between wartime and peacetime government power are built on a tenuous legal foundation. As a result, excessive restrictions on law enforcement response authority to asymmetric threats could very easily lead to an expansion of the "wartime" track to reach information perceived as critical for counterterrorism operations.

This last consideration leads to the culmination of my argument—individual liberty will be best protected by incentivizing the maximization of the "law enforcement" counterterrorism track, and minimizing the incentives to resort to the "wartime" track. In specific relation to access to data, "big" or "small," ensuring a fair balance between individual privacy and lawful government access to data will incentivize the use of the individual cause and warrant process for authorizing such access. As the Supreme Court noted in its seminal surveillance opinion, *United States v. United States District Court* (*Keith*),[24] imposition of the neutral magistrate between the zealous government agent and the individual is a vital safeguard against arbitrary government power.[25] But as will be explained below, that same case opened the door to expansive assertions of wartime surveillance power that would nullify the protective benefit of that authorization process.

I. FOURTH AMENDMENT REASONABLENESS AND THE BALANCE OF INTERESTS

Assessing the legality of government efforts to surveil "dark" spaces, whether motivated by law enforcement or counterterrorism interests, must begin with the Fourth Amendment. In one of my previously published articles, which has since evolved into a chapter for the book, *The Cambridge Handbook of Surveillance Law*, I argue that the Fourth Amendment imposes no barrier to enactment of laws requiring feasible government access to encrypted data.[26] The focus of that chapter evolved from

---

[24] 407 U.S. 297 (1972).

[25] *Id.* at 315–22 ("Inherent in the concept of a warrant is its issuance by a 'neutral and detached magistrate.'" (quoting Coolidge v. New Hampshire, 403 U.S. 443, 453 (1971) and Katz v. United States, 389 U.S. 347, 356 (1967)); *id.* at 316–17 ("Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch. The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute." (citing *Katz*, 389 U.S. at 359–60 (Douglas, J., concurring))).

[26] *See* Corn & Brenner-Beck, *supra* note 22, at 345.

the substantial public debates surrounding the San Bernardino iPhone "incident."[27] Many critics of the government, including the aforementioned chapter's co-author, questioned the wisdom and legality of government efforts to demand access codes to the E2EE embedded in the iPhone used by the deceased terrorist in that incident.[28]

For me, this issue raised the important question of whether the government has the authority to, and ought to, require encryption designers and manufacturers to preserve the means to enable government agents to *lawfully* access private data stored on the devices they market. While many critics of such a proposal lamented the idea of government mandated "backdoor" access to private data,[29] I viewed this as a requirement to build into the encryption an actual front door.[30] In my view, backdoor access connotes clandestine or surreptitious access.[31] This, I argued, is exactly what the government will be compelled to pursue and exploit when access through a proverbial front door is impossible because there is no front door.[32] However, by creating a highly secure front door, it is possible to achieve a mutually satisfactory, balanced alternative:

> To be clear, this "split key" proposal is not a subterfuge method of creating backdoor access to data. Unlike a backdoor, which generally refers to an undisclosed vulnerability in an application or device, a front door is a well-documented and clear mechanism for both encrypting and decrypting data, whether it be data in motion (communications) or at rest (stored data). To be secure,

---

[27] The San Bernardino "incident" was a mass shooting that occurred on December 2, 2015, at the Inland Regional Center in San Bernardino, California. The U.S.-born married perpetrators, Syed Rizwan Farook and Tashfeen Malik, targeted a San Bernardino County Department of Public Health training event and Christmas party. Richard Winton, *A Year After the San Bernardino Terror Attack, the FBI Is Still Struggling to Answer Key Questions*, L.A. TIMES (Dec. 1, 2016, 2:25 PM), http://www.latimes.com/local/lanow/la-me-san-bernardino-terror-probe-20161130-story.html [https://perma.cc/XC6C-GVX9]. For the purposes of this Article, the incident is notable for the FBI's attempt to access encrypted data on Farook's Apple iPhone, a move that Apple refused to assist in, and that eventually led to federal court action between the Justice Department and Apple. Matt Zapotosky, *FBI Has Accessed San Bernardino Shooter's Phone Without Apple's Help*, WASH. POST (Mar. 28, 2016), https://www.washingtonpost.com/world/national-security/fbi-has-accessed-san-bernardino-shooters-phone-without-apples-help/2016/03/28/e593a0e2-f52b-11e5-9804-537defcc3cf6_story.html?utm_term=.cd0b9d1db91e [https://perma.cc/UU9D-Y6JR]. Ultimately, the FBI did breach the device's security software and withdrew its lawsuit. *Id.*

[28] *See* Corn & Brenner-Beck, *supra* note 22, at 337–38, 368–71.

[29] *See, e.g.*, *Issue Brief: A "Backdoor" to Encryption for Government Surveillance*, CTR. FOR DEMOCRACY & TECH. (Mar. 3, 2016), http://cdt.org/insight/issue-brief-a-backdoor-to-encryption-for-government-surveillance/ [https://perma.cc/SD2T-B7HP].

[30] *See* Corn & Brenner-Beck, *supra* note 22, at 361–62.

[31] *See id.*

[32] *Id.*

> encryption should be subject to rigorous testing. Thus, its presence should be open to the public and available for attack, both in laboratories and in the real world. This is the only real way to evaluate the trustworthiness of encryption, with vulnerabilities being corrected as they are discovered, to strengthen the protocol and its implementation constantly. Essentially, a front door is the digital equivalent of a big, ingeniously engineered lock on the only entrance to an otherwise secure building. It is a lock that has been tested by every available lock picker and found to be secure, with any identified weaknesses being constantly fixed. Such a lock is always superior to a secret entrance in the rear of a building.[33]

Such front door access would better serve the interests of both privacy and security, as each would be effectively balanced.[34] First, by "splitting" the encryption key and entrusting part of it to a neutral organization devoted to privacy protection, the individual will be provided enhanced protection by imposing a greater burden on the government to access the key.[35] Second, by requiring compliance with normal Fourth Amendment justifications and authorizations to engage in surveillance and seizure of any data, the data will be protected with no less vigilance than the protection of the home.[36]

Of course, creating a front door will inevitably facilitate government access to private data when properly and lawfully authorized. This reality is contrary to the objectives of many privacy advocates.[37] Some even argue that such a creation is, in effect, a subterfuge backdoor:

> These opponents frame efforts to preserve such access as a call for the creation of "backdoors" that can be exploited by the U.S. and any other government. They argue that the creation of backdoors will introduce unacceptable vulnerabilities in products and systems and point to examples where, in the past, such vulnerability have been exploited by hackers.[38]

---

[33] *Id.* at 362.

[34] *Id.*

[35] *Id.* at 362–63.

[36] Recent Australian legislation proposes a similar process whereby access can be legally obtained via a warrant. *See New Law Would Force Facebook and Google to Give Police Access to Encrypted Messages*, GUARDIAN (July 13, 2017, 23:14 EDT), https://www.theguardian.com/technology/2017/jul/14/new-law-would-force-facebook-and-google-to-give-police-access-to-encrypted-messages [https://perma.cc/KH7M-XLDK].

[37] *See, e.g.*, *What Is Privacy*, PRIVACY INT'L, https://www.privacyinternational.org/node/54 [https://perma.cc/9E6W-CVDK] (last visited Dec. 4, 2017).

[38] Corn & Brenner-Beck, *supra* note 22, at 361–62 (citations omitted).

As I have argued previously, such a suggestion is shortsighted, as it is this approach that actually further enables exploitation by hackers.[39] When front door access is eliminated from E2EE (or any other type of data storage), a determination that access to that data is necessary and lawful will compel government agents to work to identify, if not create, backdoor access.[40] In such situations, there are strong incentives for that access to be clandestine, because disclosing the access point will in turn alert the manufacturer to a vulnerability requiring a security patch.[41] It would be unwise for the government to reveal the backdoor, only to then disclose it.[42] As a result, an actual privacy vulnerability, subject to exploitation by non-government actors, may persist.[43]

Furthermore, it is likely that the government may identify such "backdoor" vulnerabilities even when not engaged in surveillance efforts directed against specific targets as part of overall data protection operations. Without confidence that data access could be facilitated through lawful front door access, the government would have a powerful incentive not to share this information with the manufacturer or service providers. In short, front door access incentivizes government cooperation with the private sector to identify and prevent backdoor breaches, which ultimately enhances protection of private data from unlawful or unauthorized access.[44]

Reasonable people will inevitably differ on the proper balance between privacy and public security implicated by encryption technology, as well as how encryption facilitates exploitation of "dark spaces" by dangerous and nefarious actors. However, it is legitimate that a balance between these interests should be the goal of law and policy makers. Those who argue that *no* government effort to ensure lawful access to these dark spaces can be tolerated without sacrificing essential liberty are comfortable with technological creation of impenetrable zones of privacy. While such zones will obviously maximize the protection of privacy from government intrusion, they will do so at a cost. As I argued in my prior chapter, I believe an impenetrable zone of privacy is inconsistent with the underlying rationale of the Fourth Amendment:

> Balancing the competing interests of collective societal security and individual liberty is central to the Fourth Amendment touchstone of reasonableness. The notion that the Fourth Amendment provides an individual right to an impenetrable zone of privacy

---

[39] Geoffrey S. Corn, *Averting the Inherent Dangers of "Going Dark": Why Congress Must Require a Locked Front Door to Encrypted Data*, 72 WASH. & LEE L. REV. 1433, 1445 n.44 (2015).

[40] *See id.* at 1447.

[41] Corn & Brenner-Beck, *supra* note 22, at 361–62.

[42] *See id.*

[43] *See id.*

[44] The importance of ensuring cooperation between private and government actors should not be understated. For an example of what may result were this cooperation absent, see Scott Shane, *Malware Case Is Major Blow for the N.S.A.*, N.Y. TIMES (May 16, 2017), https://www.nytimes.com/2017/05/16/us/nsa-malware-case-shadow-brokers.html.

> is therefore inconsistent with the text and judicial interpretation of the amendment. Instead, balance remains the operative concept: protection against *unreasonable* search and seizure inherently acknowledged that the people can be subjected to *reasonable* searches and seizures. In short, the amendment never imposed an absolute restraint on government surveillance, even when directed against the interests protected by the amendment's text (persons, homes, papers, and effects). Instead, the people were provided an absolute right to be secure against *unreasonable* government intrusions into those places and things protected by the Fourth Amendment.[45]

That key constitutional provision certainly does not *mandate* government action to guard against the creation of such a zone, nor does it *require* the government to tolerate such zones.[46] Thus, from a regulatory perspective, the Fourth Amendment is probably best understood as neutral on the question of whether government should seek to mandate preservation of access to encrypted zones of privacy.[47]

But what the Fourth Amendment has historically tolerated—*reasonable* government measures to investigate and discover crime and other threats to public security—should be instructive in this debate.[48] Reasonableness, after all, is as the Supreme Court reminds us, the "touchstone" of the Fourth Amendment.[49] That touchstone of reasonableness, in turn, is consistently defined by balancing individual privacy with societal interests in effective law enforcement.[50] With the exception of dangerous medical procedures to recover evidence from within a suspect's body,[51] even the most carefully protected zone of privacy—the home—is subject to government intrusion when properly authorized.[52] If the most fundamental source of protection from government intrusion into a citizen's privacy is defined by a reasonable balance between privacy and security, advancing this balance should be the ultimate objective of lawmakers addressing the difficult question of how to deal with "dark spaces." Requiring preservation of encryption keys to facilitate lawful government access to private data is, in my view, a rational manifestation of this balance of interests. In

---

[45] Corn & Brenner-Beck, *supra* note 22, at 344.

[46] *See id.*

[47] *See id.*

[48] *See* Florida v. Jimeno, 500 U.S. 248, 250–51 (1991).

[49] *Id.* at 250.

[50] *E.g.*, Riley v. California, 134 S. Ct. 2473, 2482–84 (2014) (tracing the Court's construction of "reasonableness" and tying it to the need to protect officer safety).

[51] Winston v. Lee, 470 U.S. 753, 767 (1985) (holding that trying to remove a bullet from suspect's body was unreasonable under the Fourth Amendment).

[52] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

contrast, allowing for the continued creation and enhancement of technology that seeks to create impenetrable zones of privacy distorts this balance.

Ultimately, there are only three virtually undeniable constants in this debate.[53] First, the market will continue to incentivize the development of encryption technology that frustrates, and ideally prevents, government access to private communications.[54] Second, while these innovations will be intended to preserve the privacy of law abiding citizens, the dark spaces they create will offer exploitation opportunities for individuals and groups engaged in activities that threaten society.[55] And third, the government will constantly endeavor to access these dark spaces, precisely because of the risks inherent in allowing such exploitation.[56] Furthermore, the nature of national security threats, most notably terrorist threats targeting the U.S. homeland, have magnified the government's interest in penetrating these spaces.[57]

II. ASYMMETRY AND THE ADAPTIVE ENEMY

Concern over feasible access to encrypted communications is no longer simply a question of balancing privacy against the interests of effective law enforcement. Today, the risks attendant with "dark space" communications transcend criminal threats and are inextricably intertwined with counterterrorism efforts.[58] This should come as no surprise. The United States is engaged in an ongoing armed conflict against multiple transnational terrorist organizations.[59] While the notion that response to this threat qualifies as an armed conflict remains controversial for many international law experts, the fact remains that the U.S. perceives the nature of the threat posed by both al-Qaeda and ISIS as transcending that of ordinary criminal activity.[60] Instead, the national decision to treat the ongoing battle against these threats as an armed conflict indicates a willingness to use expanded means and legal authorities to disrupt and disable these groups.[61]

---

[53] *See* Jaffer & Rosenthal, *supra* note 20, at 313–17.

[54] *See id.* at 303, 313.

[55] *See id.* at 315–17.

[56] *See id.* at 296–98.

[57] *See Read the Full Testimony of FBI Director James Comey in Which He Discusses Clinton Email Investigation*, WASH. POST (May 3, 2017), https://www.washingtonpost.com/news/post-politics/wp/2017/05/03/read-the-full-testimony-of-fbi-director-james-comey-in-which-he-discusses-clinton-email-investigation/?utm_term=.0bdd2a85fee1 [https://perma.cc/M2VR-P8BT].

[58] *See* Stephanie Condon, *Intelligence Officials Warn of Threats on "Dark" Internet*, CBS NEWS (June 3, 2015, 1:57 PM), https://www.cbsnews.com/news/intelligence-officials-warn-of-threats-on-dark-internet [https://perma.cc/RT8Q-EP3K].

[59] *See* WATKIN, *supra* note 12, at 4–9.

[60] *See* Vanda Felbab-Brown, *Afghanistan's Terrorism Resurgence: Al-Qaida, ISIS, and Beyond*, BROOKINGS (Apr. 27, 2017), https://www.brookings.edu/testimonies/afghanistans-terrorism-resurgence-al-qaida-isis-and-beyond/ [https://perma.cc/Q2BF-WT96].

[61] *See* THE WHITE HOUSE, NATIONAL STRATEGY FOR COUNTERTERRORISM 6, 11 (2011)

Of course, these enemies do not engage in and employ analogous debates or handwritings over the appropriate legal framework for their terrorist activities. Instead, they embrace tactics that constantly seek to exploit enemy vulnerabilities in order to offset the superior material and information capabilities of their opponents—a phenomenon characterized by the term, "asymmetric warfare."[62] Interestingly, there is no consensus definition of asymmetric warfare.[63] However, as the following summary indicates, it generally refers to conflict between conventionally disparate enemies, with the inferior enemy seeking to offset its weakness by identifying and exploiting vulnerabilities of the conventionally superior opponent:

> Asymmetric warfare is generally understood to be a conflict in which the strengths and sizes of the opponents do not mirror each other. The side with the conventional disadvantage is probably incapable of winning through direct, conventional warfare. It must seek victory through other methods that exploit weaknesses in the superior conventional power's capacity to prevail. Examples include the Maoist Peoples' War against the Imperial Japanese Army, the Vietnamese dau trahn strategy in the First and Second Indochina Wars, and al-Qaeda's tactics in the WOT [(War on Terror)].[64]

So characterized, there is nothing new about asymmetric tactics, which have been part of military theory and doctrine dating back to the writings of Sun Tzu.[65] However, the struggle against today's transnational terrorist threats has resurrected the focus on how to effectively address asymmetric threats, threats that challenge our national security capabilities well beyond the "battlefield."[66] A Rand Report explains the characteristics and challenges associated with this modern permutation of asymmetric warfare:

[hereinafter 2011 TERRORISM STRATEGY]; David A. Wallace, *Battling Terrorism Under the Law of War*, 87 MIL. REV. 101, 101–02 (2007).

[62] U.S. DEP'T OF THE ARMY, FIELD MANUAL 3-05.130, ARMY SPECIAL OPERATIONS FORCES UNCONVENTIONAL WARFARE J-3 (2008) [hereinafter ARMY, FIELD MANUAL 3-05.130].

[63] *See* JOINT CHIEFS OF STAFF, JOINT PUBLICATION 1-02, DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 17 (2016) (defining "asymmetric," but failing to define "asymmetric warfare").

[64] ARMY, FIELD MANUAL 3-05.130, *supra* note 62, at J-3–J-4.

[65] *See* SUN TZU, THE ART OF WAR: COMPLETE TEXTS AND COMMENTARIES 88–89, 116–18 (Thomas Cleary trans., 2003) (discussing tactics against formless enemies and those with superior advantages).

[66] *See generally* AMICHAY AYALON & BRIAN MICHAEL JENKINS, RAND CORP., WAR BY WHAT MEANS, ACCORDING TO WHOSE RULES? THE CHALLENGE FOR DEMOCRACIES FACING ASYMMETRIC CONFLICTS: PROCEEDINGS OF A RAND-ISRAEL DEMOCRACY INSTITUTE WORKSHOP, DECEMBER 3–4, 2014, at 39–41 (2015), https://www.rand.org/pubs/conf_proceedings/CF334.html [https://perma.cc/Y8VX-4WQ6].

The legal dimension of asymmetric warfare is often called "lawfare." This is a relatively new area because the nature of modern warfare has changed dramatically from that of the "classical" wars of the past. In classical warfare, the enemy is visible, and soldiers are easily identifiable by uniform and openly carry weapons. The use of lawfare is part of the larger pursuit of legitimacy.

By contrast, in asymmetric warfare, the enemy is usually invisible, hiding among the civilian population, often in densely populated areas. Lethal attacks are often launched from civilian facilities. There may be no means to distinguish combatants from the civilian population.

In classical warfare, a democratic nation's obligation and responsibility is to conduct the war according to the rules of war—especially the principle of distinction between combatants and civilians.

When it comes to asymmetric warfare, the opponent often targets civilians, not only ignoring the rules of war but deliberately doing so as part of an overall strategy against the democratic state.

In classical warfare, the ultimate goal of both sides is to defeat the enemy with respect to its capabilities to use military power. In asymmetric warfare, the opponent's goal is not to defeat the state's armed forces but rather to make the civil society so terrified and concerned that it will pressure politicians to withdraw from the state's positions or abandon its policy aims, thereby losing the war not through the battlefield but through determination of the democracy not to continue fighting.

In classical warfare, the territorial and temporal limits of the conflict are relatively defined. The nature of asymmetric warfare is much more amorphous. It is not limited to a certain territory or distinct timeline.

In classical warfare, the enemy's fighters are essentially anonymous: It is not important to know the name of the enemy's soldier or commander before attacking him.

When it comes to asymmetric warfare, in many cases, it is crucial to know the opponent and to have very personal and detailed

information as a precondition for determining the legitimacy of a strike.

These new features are different from the set of assumptions that were the basis for the laws of war, especially international humanitarian law. These laws are the basis of the legal norms, binding democratic nations to conduct their military power accordingly.

This differentiation, combined with the emerging power and influence of international tribunals, is known as lawfare.

Lawfare is often used as a negative term, suggesting manipulation, although it is not limited to that. Ironically, it is an area in which the democratic state and its officials feel vulnerable. In contrast, the opponent often deliberately violates the norms while simultaneously using them to weaken democratic nations. Lawfare is used to counter the weapons of the democratic state by exploiting its own laws and judicial systems. It focuses on government and personal liability.

Because asymmetrical warfare takes place in densely populated areas, it inevitably generates more grounds for legal action. While nonstate adversaries typically do not comply with international humanitarian law, as already noted, they will simultaneously use that law to undermine the motivation and legitimacy of their democratic state foes.

. . . .

There are inherent difficulties in applying the norms of international humanitarian law to asymmetric warfare. Applying the concept of *proportionality* is next to impossible and provides no guidance to the commanders on the ground, since it comes without clear guidelines. It is also difficult to apply the fundamental principle of *distinction* in a civilian environment, since the entire battlefield is often a civilian area, making it nearly impossible to distinguish between combatants and civilians. Moreover, the application of the principle of *military necessity* is problematic when it relies heavily on intelligence and other secret evidence. Finally, asymmetric warfare presents challenges to efficiently striking the opponent without violating the principle of *perfidy*. Effective warning—for example, roof knocking—weakens the

> chances of a successful military mission and places soldiers at additional risk. Other challenges include striking political or religious targets, regardless of whether they are also being used to support active military operations. What about individuals like Hamas leader Ismail Haniye? Or how should armies treat bridges or electricity? In World War II, such targets were bombed for obvious military reasons. In asymmetric warfare, they may be considered civilian facilities.
>
> Consequently, the challenge is how to adjust international humanitarian law to apply to modern asymmetric wars. There needs to be legal recognition of the constant state and timeless nature of armed conflict against nonstate adversaries. There needs to be legal application of the principle of self-defense against nonstate adversaries when there is no other alternative (for example, in failed states). Given that liberal democracies are often on the front line in the fight against nonstate adversaries, there needs to be a flow of information among them as well.
>
> Furthermore, it is necessary to acknowledge the role that intelligence plays in winning the war and to determine the "military necessity" and the key element of intelligence for the principle of *distinction*. Also, wider legal tools and wider public control over intelligence agencies should be considered.
>
> It is important to develop a publicly available code of conduct for certain military actions, such as targeted killings. It is important to know who is making the decisions and under what guidelines and circumstances targeted killings are allowed. Sharing more intelligence publicly assists in efforts to win the imagefare battle.[67]

As indicated in the RAND Report, one aspect of asymmetric terrorist tactics that creates especially difficult challenges for law-abiding nations is exploitation of the law to gain tactical advantage.[68] Whether on a conventional battlefield in Iraq, an unconventional battlefield like Afghanistan, or the enemy's "homeland," contemporary enemies look for opportunities created by their opponent's compliance with legal obligations.[69] This aspect of asymmetry may not be completely new, but it is

---

[67] *Id.*
[68] *See id.*
[69] *See id.* at 40.

more pervasive than ever before.[70] This may be a consequence of the increasing role law plays in defining the legitimacy of national security actions. In fact, the concept of legitimacy is now included in some U.S. military doctrine as a principle of war, alongside such time-tested principles as mass, offensive, and economy of force.[71] As a result, democracies face an increasingly difficult challenge of developing and implementing national security policies that are effective, not only in the immediate sense of achieving the effect on the opponent, but also in the sense that they manifest the type of commitment to law that is central to the notion of legitimacy.

This aspect of asymmetry intersects directly with the issue of government surveillance access to "dark spaces." Remotely radicalized, homegrown terrorists are assessed as among the most significant terrorist threats faced by Western nations.[72] Furthermore, attacks in Paris, Brussels, and other major cities demonstrate the risk of small, well-organized attack cells operating in relative plain sight.[73] Whether it is a lone wolf, or a small cell of organized operatives, communication is obviously essential for their success. And, because it is no mystery that the government is constantly seeking to identify and preempt terrorist attacks, it must be self-evident to such individuals that identification and exploitation of dark communication zones will substantially enhance their likelihood of success. Investigations into several attacks, such as the ISIS Paris bombings and the Brussels airport bombing, indicate that operatives relied on WhatsApp for vital communications.[74]

The ready availability of E2EE with no built in front door access will almost certainly be viewed by those engaged in terroristic activities as the communications method of choice. Like all aspects of asymmetric warfare, they will seek to exploit what is viewed as a self-inflicted vulnerability to the maximum extent. The more confident they are in the immunity of their communications from timely government surveillance, the more likely it is they will rely on such dark spaces. But this also means that the government is all that more likely to increase efforts to penetrate such spaces. And this really frames the ultimate question in the encryption debate: does increasing

---

[70] *See id.* at 41–44.

[71] JOINT CHIEFS OF STAFF, *supra* note 9, at I-2 ("Since the establishment of the Joint Chiefs of Staff in 1947, joint doctrine has recognized the nine principles of war. Subsequent experience from a wide variety of irregular warfare (IW) situations has identified three additional principles—restraint, perseverance, and legitimacy.").

[72] *See generally* Toni Johnson, *Threat of Homegrown Islamist Terrorism*, COUNCIL ON FOREIGN REL., https://www.cfr.org/backgrounder/threat-homegrown-islamist-terrorism [https://perma.cc/L67S-W9ZG] (last updated Sept. 30, 2011).

[73] *See* Zainab Fattah & Ladane Nasseri, *Here Are the Major Terror Attacks in Europe, From Paris to Oslo*, BLOOMBERG (June 19, 2017, 11:40 AM), https://www.bloomberg.com/news/articles/2017-06-19/here-are-the-major-terror-attacks-in-europe-from-paris-to-oslo [https://perma.cc/2D6T-SJR2].

[74] Sebastian Rotella, *ISIS via WhatsApp: 'Blow Yourself Up, O Lion*,*'* FRONTLINE (July 11, 2016), http://www.pbs.org/wgbh/frontline/article/isis-via-whatsapp-blow-yourself-up-o-lion/ [https://perma.cc/SD38-6NBP].

the difficulty of lawful government access ultimately advance or compromise legitimate privacy interests? The answer to this question may be derived in part from the multipronged legal framework the U.S. relies on for counterterrorism operations.[75]

III. COUNTERTERRORISM: "FIGHTING AT THE LEGAL BOUNDARY"

In his award-winning book, *Fighting at the Legal Boundaries*, Brigadier General (Retired) Kenneth Watkin, the former Judge Advocate General of the Canadian Armed Forces, explores the many legal uncertainties associated with military operations against non-state threats.[76] Central to his thesis is that the nature of the threats posed by these groups straddles the line between criminal law enforcement and military armed conflict[77]:

> A particular challenge for international law is how to deal with conflicts that are fundamentally "criminal insurgencies." In some instances these insurgencies are conducted by gangs for which "*[d]rug trafficking organization* is no longer a sufficient term for them; they are a *criminal paramilitary complex*." There often is little difference in terms of organization between such paramilitary gangs and insurgent groups. Taken together, these new threats have been described as "*non*state" (e.g., gangs, insurgents, drug traffickers, transnational criminal organizations, terrorists, warlords), where conflict "thrive[s] in 'ungoverned or weakly governed space' between or within various host countries," and *intra*state, "which tends to involve direct and indirect conflict between state and nonstate actors." Such conflicts challenge not only traditional notions of what constitutes armed conflict but also how amendable the resulting violence is to a law enforcement response. As a result, "[t]he power to deal with these kinds of situations is no longer hard combat firepower or even the more benign police power." These situations of insecurity challenge traditional notions of the dividing line between armed conflict and ordinary law enforcement.[78]

---

[75] *See generally* THE LAW OF COUNTERTERRORISM (Lynne K. Zusman ed., 2011) (providing a number of perspectives on what "counterterorism" means and the role that the law plays in the United States' effort to combat transnational terrorism).

[76] *See* WATKIN, *supra* note 12, at 5–6, 10, 16, 23. Watkin's comprehensive work was the winner of the 2017 Francis Lieber Prize. *See* OXFORD U. PRESS, https://global.oup.com/academic/product/fighting-at-the-legal-boundaries-9780190457976?cc=us&lang=en& [https://perma.cc/7W4N-FQLF] (last visited Dec. 4, 2017).

[77] *See* WATKIN, *supra* note 12, at 6.

[78] *Id.* at 6–7 (citations omitted).

For Watkin, this requires a careful and deliberate strategic and operational assessment of if and when resort to authorities restricted to armed conflict may be legitimately invoked.[79]

The United States has been fighting at this "legal boundary" since it initiated the military response to the September 11 terrorist attacks (and according to government prosecutors at Guantanamo, even before that date).[80] Characterizing this response, or at least aspects of this response, as an armed conflict is a position that has been embraced by all three branches of the federal government.[81] This characterization was of profound significance. By doing so, the United States invoked a range of counterterrorism response authorities that would otherwise not have been available pursuant to a peacetime law enforcement characterization.[82]

Attacking individuals with lethal force and indefinite preventive detention are probably the most notable (and, in the view of some notorious) manifestations of this expansion of authority.[83] These two aspects of U.S. counterterrorism policy are not directly related to the issue of "dark space" surveillance. However, the broader significance of these policies is that they reflect a reality that transcends these specific measures, the reality that Brigadier General Watkin highlights in his book: threats that straddle the legal boundary between law enforcement and "war" may incentivize expansive invocations of international law derived war powers by States struggling to disrupt or disable these threats.[84]

The invocation of war powers to respond to the 9/11 terrorist attacks did impact the government's legal theory related to surveillance.[85] In fact, one of the most

---

[79] *See id.* at 329–31.

[80] *See* Morris Davis, Op-Ed, *Here's Why I Resigned as the Chief Prosecutor at Guantanamo*, L.A. TIMES (Oct. 4, 2017, 4:00 AM), http://www.latimes.com/opinion/op-ed/la-oe-davis-why-i-resigned-as-chief-prosecutor-for-military-commissions-guantanamo-20171004-story.html [https://perma.cc/6FQV-BM4C]; *see also* Kyndra Rotunda, *Applying Geneva Convention Principles to Guantánamo Bay*, 43 U. RICH. L. REV. 1067 (2009).

[81] *See* Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001) (congressional declaration of armed conflict); Hamdan v. Rumsfeld, 548 U.S. 557, 630 (2006) (judiciary treating issue as armed conflict); 2011 TERRORISM STRATEGY, *supra* note 61, at 3 (executive branch addressing terrorist threat as armed conflict).

[82] Philip M. Bridwell & Jamil N. Jaffer, *Updating the Counterterrorism Toolkit: A Brief Sampling of Post-9/11 Surveillance Laws and Authorities*, *in* THE LAW OF COUNTERTERRORISM 231, 237–38 (Lynne K. Zusman ed., 2011).

[83] *See, e.g.*, Jack Goldsmith, Opinion, *Obama's Breathtaking Expansion of a President's Power to Make War*, TIME (Sept. 11, 2014), http://time.com/3326689/obama-isis-war-powers-bush/ [https://perma.cc/P4AR-9MDV]; Brendan Fischer & Lisa Graves, *International Law and the War on Terror*, WATSON INST. FOR INT'L & PUB. AFF. (2011), http://watson.brown.edu/costsofwar/files/cow/imce/papers/2011/International%20Law%20and%20the%20War%20on%20Terror.pdf [https://perma.cc/5SVD-XAU9].

[84] *See* WATKIN, *supra* note 12, at 22–23.

[85] *See* U.S. DEP'T OF JUSTICE, A REVIEW OF THE DEPARTMENT OF JUSTICE'S INVOLVEMENT WITH THE PRESIDENT'S SURVEILLANCE PROGRAM (U) 1–2 (2009) [hereinafter PSP REPORT]; *see also* Bridwell & Jaffer, *supra* note 82, at 231.

controversial policies adopted by the Bush administration was the Presidential Surveillance Program (PSP), referred to as "Stellar Wind" in its classified form.[86] This program involved large-scale communications surveillance that included within its scope telephone calls with one party in the United States, potentially involving U.S. persons, based solely on repeated, short-duration Executive Branch authorizations.[87] The fact that the government engaged in such surveillance was not necessarily controversial. What was controversial was the decision to implement the program outside of the existing framework for review and authorization for such surveillance activities established by the Foreign Intelligence Surveillance Act (FISA).[88] FISA, enacted by Congress in 1978, requires judicial authorization for foreign intelligence surveillance activities, which include surveillance directed against international terrorist organizations.[89]

As justification for implementing the program outside of the FISA framework, the President and his legal advisors asserted multiple authorities over the course of PSP's existence.[90] The most notable of these was the constitutionally vested authority as Commander in Chief of the armed forces:

> Article II, Section 2 of the Constitution, which was one of the primary authorities cited in the Presidential Authorizations in support of the legality of the Stellar Wind program, provides in relevant part:
>
> > The President shall be Commander in Chief of the Army and Navy of the United States, and of the Militia of the several States, when called into the actual Service of the

---

[86] *See* PSP REPORT, *supra* note 85, at 28, 406–07. *See generally* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c (2012). The program was and is now referred to by numerous names, as set forth in the Justice Department's assessment in the PSP Report:

> The President and other Administration officials labeled the NSA collection of information that was publicly disclosed as "the Terrorist Surveillance Program," although this name was sometimes used within the Intelligence Community to refer to the entire Stellar Wind program. The program was also referred to by other names, such as the "Warrantless Wiretapping Program" or the "NSA Surveillance Program." As discussed above, the technical name for the program, and the term we generally use throughout this report, is the Stellar Wind program.

PSP REPORT, *supra* note 85, at 3.

[87] *See* PSP REPORT, *supra* note 85, at 14 n.16, 16, 28 (stating that between October 4, 2001, and February 1, 2007, forty-three of these authorizations were issued).

[88] *See* CORN ET AL., *supra* note 18, at 198 (discussing how FISA differed from existing Title III framework for warrants).

[89] *See* 50 U.S.C. §§ 1801–1813; CORN ET AL., *supra* note 18, at 196–258 (providing a detailed discussion of intelligence exploitation).

[90] *See* PSP REPORT, *supra* note 85, at 7–18.

> United States; he may require the Opinion, in writing, of the principal Officer in each of the executive Departments, upon any Subject relating to the Duties of their respective Offices . . . .[91]

Because the nation was engaged in an armed conflict with al-Qaeda, gathering of intelligence against this "enemy" threat was, according to the President, a traditional war power requiring no statutory authorization.[92]

Public and congressional reaction to this program led to its termination, and subsequent surveillance efforts were conducted pursuant to FISA (which was amended several times to better accommodate counterterrorism concerns).[93] However, the assertion of a war powers-based justification for dispensing with FISA surveillance authorization requirements indicates the impact of designating counterterrorism efforts as an armed conflict. While it may be true that to date, FISA is considered sufficient to accommodate government intelligence collection and counterterrorism surveillance interests,[94] there is no guarantee that this will always be the case.

Ultimately, the intersection between counterterrorism, armed conflict, and government surveillance interests cannot be ignored when considering how to best address the risks associated with "dark spaces." So long as assertion of war powers to justify intelligence gathering and counterterrorism efforts remains a possibility, the development of technology that facilitates such spaces may not offer the benefits that many privacy advocates hope for. Perhaps carefully regulated access to such spaces will ultimately advance privacy interests by incentivizing government action on the "peacetime" territory of this complex legal boundary.

IV. BE CAREFUL WHAT YOU ASK FOR

If, as most anticipate, encryption development will continue to increase access to "dark spaces," the government will be confronted with a limited range of response

---

[91] *Id.* at 7 (quoting U.S. CONST. art. II, § 2); *see* Memorandum from Steven G. Bradbury, Principal Deputy Assistant Attorney Gen., U.S. Dep't of Justice, Status of Certain OLC Opinions Issued in the Aftermath of the Terrorist Attacks of September 11, 2001 (Jan. 15, 2009), https://www.justice.gov/sites/default/files/opa/legacy/2009/03/09/memostatusolcopinions01152009.pdf [https://perma.cc/U9TR-3MB4] (discussing the President's Article II authority with respect to FISA).

[92] *See* PSP REPORT, *supra* note 85, at 7–16 (containing, among other things, a timeline of the legal authorities on which the government relied at certain phases in the PSP's existence).

[93] *See* CORN ET AL., *supra* note 18, at 202, 204, 245.

[94] *See generally* James G. McAdams, III, *Foreign Intelligence Surveillance Act (FISA): An Overview*, FED. L. ENFORCEMENT TRAINING CTR., http://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf [https://perma.cc/RC6B-46RE] (last visited Dec. 4, 2017) (stating how Congress has enhanced the ability of counterterrorism agents to use FISA).

options. One option would be to simply let the market drive the technological advances in encryption, with the accordant risk of increasingly impenetrable E2EE. Another option would be to prohibit "keyless" E2EE altogether. A third option would be to seek a reasonable accommodation of the societal interest in enhanced protection for private data and the government interest in effective law enforcement and national security surveillance.

Advocates of the first option may believe that it provides the best protection against privacy compromise, either the result of unlawful government action or private intrusions. However, these advocates may not have fully contemplated the risk that foreclosing government access to data through normal, law enforcement-type modalities may push the government into pursuing extraordinary surveillance measures justified by an assertion of war powers. There is no reason to expect that the government will ignore the potential security advantages of surveillance targeted at "dark spaces."[95] Indeed, the nature of the international terrorist threats confronting the nation—threats emanating from organizations that rely heavily on commercial communications capabilities not only for command and control, but for recruiting and inciting violent terrorist actions—virtually guarantees that government counterterrorism efforts will constantly seek to access such data.

Without an ability to rely on normal law enforcement agencies and processes to engage in such surveillance, the government will not simply "give up" the effort. Instead, the incentive to invoke wartime powers and utilize all surveillance capabilities, including military capability, will be increased. Like the Bush-era PSP, a future President would need only determine that the information sought by the government was related to an enemy involved in an ongoing armed conflict with the United States. And this might not be an all that difficult finding to make. First, as has been demonstrated with the seemingly endless expansion of authority derived from the post-9/11 Authorization for Use of Military Force,[96] it has not been terribly difficult to link terrorist organizations to that authority.[97] Second, even a presidential determination that a terrorist threat fell beyond the scope of that authorization would not bar a President from invoking war powers as a justification for surveillance efforts.[98] Because it is now well established that international terrorist organizations may present the United States with a threat of an "armed attack," a President would be able to invoke the inherent constitutional "defensive" war power to disrupt or disable such a threat.

Of course, any president moving down this road would have to contend with the same obstacle that confronted President Bush—that even when dealing with wartime

---

[95] *See* Condon, *supra* note 58.

[96] Authorization for Use of Military Force, Pub. L. No 107-40, 115 Stat. 224 (2001).

[97] *See generally* Curtis A. Bradley & Jack L. Goldsmith, *Congressional Authorization and the War on Terrorism*, 118 HARV. L. REV. 2047, 2101–17 (2005).

[98] *See* Robert Bloom & William J. Dunn, *The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment*, 15 WM. & MARY BILL RTS. J. 147, 179–84 (2006).

threats, FISA establishes the sole means for authorizing surveillance.[99] But, this is not necessarily an insurmountable obstacle. First, President Bush never conceded a lack of constitutional authority for his program, but simply chose to acquiesce to the use of FISA as the means to obtain surveillance authorization.[100] Second, FISA may very well provide ample authority to utilize extraordinary measures to penetrate "dark spaces" to include the use of military surveillance capabilities.

So where does this leave us? In a nutshell, the proverbial unstoppable force seems to be colliding with the immovable object—encryption will continue to improve the "darkness" of "dark spaces," and the government's interest in accessing those spaces will only continue to increase. Ignoring these realities carries great peril, because it will almost certainly push the government towards more extreme measures to achieve its vital counterterrorism intelligence objectives.

The third option averts this risk and also averts the risk of granting nefarious actors a windfall of operational maneuver space. This option involves a statutory mandate that encryption build in front-door access. Congress could impose this mandate on any entity marketing encryption technology in the United States. As noted above, there is no reason to believe that such a legislative mandate would conflict with Fourth Amendment protections.[101] Instead, such a mandate can be seen as aligned with the Fourth Amendment, because it will incentivize the use of "normal" surveillance authorization methods to achieve counterterrorism and law enforcement objectives.[102]

Opponents to this third, middle-ground approach and proposed Congressional mandate "argue that the creation of back doors will introduce unacceptable vulnerabilities in products and systems and point to examples where, in the past, such vulnerabilities

---

[99] *See id.* at 160–64.

[100] PSP REPORT, *supra* note 85, at 250–51, 260. The following excerpt from the Justice Department's contribution to the PSP Report sheds light on the open-ended conclusion to the PSP:

> On December 8, 2006, the President signed what would become the final Presidential Authorization for the Stellar Wind program. The December 8 Authorization was scheduled to expire on February 1, 2007. However, Judge Howard's January 10, 2007, Orders relating to foreign and domestic selectors completed the transition of Stellar Wind's communications and meta data collection activities from Presidential Authorization to FISA authority. Bradbury told the OIG that because it was believed that Judge Howard's Orders, particularly the foreign selectors Order, provided the NSA sufficient flexibility to conduct content collection, it was not necessary to renew the December 8, 2006, Presidential Authorization.
>
> Therefore, on February 1, 2007, the Presidential Authorization for the Stellar Wind program officially expired.

Id. at 250–51.

[101] *See supra* Part I.

[102] *See supra* Part I.

have been exploited by hackers."[103] This concern is legitimate; however, as noted above, such a concern is not sufficient to necessitate allowing unrestricted encryption development.[104] First, measures could be adopted to mitigate the risk of government abuse of surveillance power, such as a split-key concept outlined earlier that provides a prophylactic protection against improper government access to encrypted data.

Second, the ready availability to lawful access will obviously incentivize government reliance on judicial authorization, thereby enhancing protection against improper government access. Finally, even if it is assumed that no measure can guarantee protection against unlawful government surveillance, that risk is no different than any other type of government surveillance. After all, nothing prevents government agents from unlawfully entering and searching a home. Nonetheless, homes have doors that facilitate access. It is therefore odd to assert that protection against unlawful government access to data necessitates a "doorless" container, whereas the home itself includes an analogous inherent risk.

Ultimately, facilitating lawful and judicially authorized government access to encrypted data will enhance and not degrade privacy protection. It will incentivize government/private information sharing on security breaches; it will subject the government to the process of surveillance authorization that exemplifies "reasonableness" pursuant to the Fourth Amendment;[105] and it will disincentivize pursuit of extraordinary extrajudicial methods to access such data. In an era of virtually endless armed conflict against transnational terrorist organizations,[106] this latter consideration deserves more attention. Like the debate over expanding the public safety exception for terrorist questioning without a *Miranda* warning,[107] it is essential to recognize that the "military track" profoundly impacts the cost/benefit analysis. When the cost of policy decisions is not necessarily an increase in individual liberty, but a shift of government authority to a wartime military track, it should cause significant pause.

CONCLUSION

As I have indicated throughout both this Article and in my earlier chapter, there are numerous advantages to a lawful "front door" access point to encrypted information. First, such an access method is the appropriate approach for striking a balance with the Fourth Amendment reasonableness requirement. Secondly, the nature and frequency of now constantly emerging asymmetric threats necessitates adopting an approach that denies these perpetrators the forum in which to enjoy completely

---

[103] Corn, *supra* note 39, at 1445–46 (citations omitted).

[104] *See supra* Part I.

[105] *See supra* Part I.

[106] *See* WATKIN, *supra* note 12, at 4–9.

[107] *See generally* Geoffrey Corn & Chris Jenks, *Strange Bedfellows: How Expanding the Public Safety Exception to* Miranda *Benefits Counterrorism Suspects*, 41 FORDHAM URB. L.J. 1 (2013).

secret communication. But my primary point of this Article is to iterate an additional consideration—that the increasingly tenuous line between wartime and peacetime government power has created an atmosphere where any excessive restrictions of law enforcement response authority risks an expansion of the wartime response authority. Therefore, for individual liberty to be protected, law enforcement counterterrorism response authority must be maximized.