

LONG WARS OF POLITICAL ORDER—
SOVEREIGNTY AND CHOICE:
THE FOURTH AMENDMENT AND
THE MODERN TRILEMMA

Harvey Rishikof †

INTRODUCTION	587
I. POLITICAL ORDER: A U.S. JUDICIAL CONTEXT AND THE BROADER MODERN TRILEMMA	590
II. ARE THERE ANY PUBLIC POLICY LESSONS FROM THE WAR ON DRUGS?.....	602
III. IS THE INSTITUTIONAL SOLUTION REORGANIZATION? – DHS? DNI? MI5?	606
IV. SHOULD AMERICA HAVE AN MI5?	611
CONCLUSION: SOVEREIGNTY AND CHOICEt	615

INTRODUCTION

In the opening of Graham Allison’s book, *Nuclear Terrorism*, Allison describes how the Central Intelligence Agency director, George Tenet, at the Presidential Daily Intelligence Briefing on October 11, 2001, informed President Bush that he had information that Al Qaeda had acquired a stolen Russian ten-kiloton nuclear bomb and that the source of the information believed the weapon was in New York City. According to Allison, in a moment of gallows humor, a staffer quipped that the terrorists could have wrapped the bomb in one of the bales of marijuana that are routinely smuggled into cities like New York.¹ The report proved to be false – this time.²

In fact, other semi-criminal enterprises such as arms trafficking have perfected the process of evading borders. For example, Victor Bout, by most accounts the world’s largest arms trafficker, has amassed a vast arsenal of planes, pilots and crews and created a transportation net-

† Chair, Department of National Security Strategy at the National War College. *Previous positions held:* Legal Counsel to the Deputy Director of the FBI; law clerk to the Honorable Leonard I. Garth (3rd Cir.); AA to Chief Justice William H. Rehnquist; Supreme Court Fellow; Dean, Roger Williams University School of Law. The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the National War College, the Department of Defense, or the U.S. Government.

¹ GRAHAM ALLISON, *NUCLEAR TERRORISM*, 1-2, (2004).

² To see the effects of a ten-kiloton nuclear bomb, see www.nuclearterror.org.

work or “tubes” with pilots earning an average of \$10,000 per shipment.³ Peter Landesman, an investigative journalist, has pointed out that arms traffickers inherited not only the Soviet Union’s cold-war weapons supply but also its fully operational systems of clandestine transport, replete with money channels, people who understood how to use them, and, most important, established shipping pipelines.⁴ Robert Gelbard, assistant secretary of state for international narcotics and law enforcement under President Clinton, described such networks to Landesman as “tubing.”⁵ Gelbard noted that the “tubes” can carry different kinds of things – “drugs, humans, money – or weapons.”⁶

The tubing process is described as follows:

Arms traffickers use what looks like legitimate business activity to disguise the smuggling. Weapons shopping lists are quietly passed through webs of people who fill orders, often for cash on delivery. Usually, the first link in the chain is military; bribes are paid to officials and officers to look the other way, or soldiers are paid to play warehouse stock clerks. Sometimes crates of weapons are labeled perishable fruit. Or waiting aircrews switch cargo at “refueling” stops. A pilot might fly into an airport under one registration number and fly out under a different one. Or he might start off on an openly planned flight from, say, Ostend to Peru, then double back and dogleg south to a war zone in West Africa. Payments are wired from a buyer’s shell company into a seller’s shell, often in money-laundering havens like the Isle of Man or the Caymans or Dubai, or money is wired to quasi-legitimate cargo companies. Sometimes weapons are simply traded for bags of cash or sockfuls of diamonds.⁷

Victor Bout was a master of tubing and had ties to Central Africa, Southern Africa, Nigeria, the Emirates, Belgium, and the Ukraine.⁸ Between 1992 and 1998 approximately \$32 billion of large and small-scale Ukrainian weaponry and ammunition disappeared.⁹ Customers ranged from Iraq, Iran, Somalia, Yemen, and Pakistan.¹⁰ There is no effective

³ Peter Landesman, *Arms and the Man*, N.Y. TIMES, Aug. 17, 2003, § 6 (Magazine), at 28.

⁴ *Id.*

⁵ *Id.* at 5.

⁶ *Id.*

⁷ *Id.* at 6.

⁸ *Id.* at 4.

⁹ *Id.*

¹⁰ *Id.* at 5.

“legal architecture” to regulate the arms network that operates “across international borders in the political twilight,” because each country views arms trafficking as one of national security and therefore as a question of national sovereignty.¹¹ The arms trafficking business is further complicated when governments, for geopolitical or national security reasons, support proxy armed political movements; the result is “killers, traffickers, smugglers and criminals” enlisted to fight a “just war.”¹² In the words of a former U.S. government official, there is a “disposal problem” – for such a strategy, “Ask Manuel Noriega. He’d know.”¹³ The disposal problem is the unintended consequences of these clandestine businesses and the operatives and institutional networks they create for powers that employ the proxies.

For many U.S. strategists, this is how the War on Drugs meets the Global War on Terrorism (“GWOT”), the fear that the smuggling routes that have been perfected over the last three decades by drug cartels or other quasi-criminal groups will be exploited by terrorist groups to deliver a nuclear, dirty, chemical, or biological bomb that will kill tens of thousands of Americans on the homeland.¹⁴ The drug smugglers have demonstrated over and over again that our borders are not secure. Moreover, although not often remembered, in 1972, three Americans hijacked Southern Airways Flight 49, circled the Oak Ridge nuclear research reactor in Tennessee, threatened to crash the plane, demanded a ransom of \$2 million from the airlines, and finally were imprisoned in Cuba.¹⁵ The threat of a combination of a terrorist act and a nuclear, biological, radiological, or chemical (“NBRC”) incident fuels our foreign policy and guides our domestic homeland defense.¹⁶ This is not to say that two individuals with a high-powered rifle, randomly shooting innocent Americans, cannot terrorize our local populations, but it is a matter of scale and degree when NBRC issues are involved.¹⁷

For other strategists, the critical tie between terrorism and drugs is money. The most recent manifestation of this tie is the support for the

¹¹ *Id.* at 10.

¹² *Id.* at 7.

¹³ *Id.*

¹⁴ See ALLISON, *supra* note 1, at 7.

¹⁵ *Id.*

¹⁶ Referred to as the “Cheney Doctrine;” When thinking about a low probability, high impact event, Cheney is reported to have said when news reached the White House that Bin Laden had been meeting with Pakistani scientists about the nuclear bomb that “If there’s a one percent chance that Pakistani scientists are helping al Qaeda build or develop a nuclear weapon, we have to treat it as a certainty in terms of our response.” See Barton Gellman, *The Shadow War, in a Surprising New Light*, WASH. POST, June 20, 2006, at C1 (reviewing Ron Suskind’s *THE ONE PERCENT DOCTRINE*).

¹⁷ See Margaret Neighbour, *Washington sniper sentenced to death*, THE SCOTSMAN, Mar. 10, 2004, at <http://news.scotsman.com/topics.cfm?tid=584&id=276872004>.

heroin trade by the Taliban in Afghanistan.¹⁸ Interestingly, when the Taliban was in power, it aimed to reduce the drug trade. Now as an insurgency movement, the Taliban leaders have understood the benefits of drugs as a source of income to support the struggle against the Karzi government and its allies.¹⁹ Drug lords are also extremely proficient at “money laundering” and have mastered the technique of moving tens of millions of dollars around the globe.²⁰ Finally, narco-based gangs pursue their own form of “narco-terrorism” or, as defined in the Drug Enforcement Agency strategic plan, terrorism conducted to further the aims of drug traffickers, including “assassination, extortion, hijackings, bombings, and kidnappings directed against judges, prosecutors, elected officials, or law enforcement agents and the general disruption of a legitimate government to divert attention from drug operations.”²¹

All governments have found, however, that it is hard to declare war on a tactic (terrorism), or a plant or chemical (drugs), or even a condition (poverty), in the traditional sense of the law of armed conflict. Metaphors are helpful in rallying support for public policies but often can mislead when the metaphors do not accurately fit the problem. The challenges posed by drugs and terrorism stem from social and political forces and are more similar to protracted struggles or wars for “political order” than to armed conflict. The foes in the GWOT oppose our foreign policy, the rise of globalism, and the principles of a liberal democratic state. The foes in the War on Drugs provide a service and product that American and European citizens are demanding. Citizen who do not participate in our economy of opportunity are the objects of the War on Poverty. These are not wars in the traditional sense – these are long-term public policy programs requiring multi-faceted approaches by sovereign states providing legitimate choices to their own citizens.

I. POLITICAL ORDER: A U.S. JUDICIAL CONTEXT AND THE BROADER MODERN TRILEMMA

In any struggle to establish political order and maintain public safety, debates will ensue over whether it is wiser to view the threat of terrorism or even drugs as a “law enforcement” problem or a “military

¹⁸ See Ahmed Rashid, *Afghanistan: On the Brink*, 53 N.Y. REV. OF BOOKS, June 22, 2006, available at <http://www.nybooks.com/articles/19098>.

¹⁹ Though some have argued that the Taliban cut the production of heroin and then sold the warehoused contraband at inflated prices for profit and gain. Interview by Harvey Rishikof in Washington, D.C. (August 2006).

²⁰ See Tim Padgett, *Banking On Cocaine*, 151 TIME LATIN AMERICA, June 1, 1998, available at http://www.time.com/time/magazine/1998/int/980601/latin_america.banking_on5.html.

²¹ U.S. DEP'T OF JUSTICE, DRUG ENFORCEMENT ADMINISTRATION, STRATEGIC PLAN, FY 2003-FY 2008 32. (on file with the author).

one.”²² The facile answer is both. However, which paradigm ultimately frames the approach may have far-reaching consequences for the personal autonomy citizenship issue. A state that emphasizes the military instrument in a domestic context will increasingly have a martial emphasis and has a higher probability of encouraging the role of the military in all of its critical domestic institutions. A law enforcement emphasis may provide more restraint depending on how effectively personal autonomy rights are respected and policed by the authorities in charge. Greater public and personal surveillance and decreased private autonomy will inevitably follow from either paradigm—military or law enforcement. The fundamental questions for both paradigms are what are the checks and balances on the government and how are citizens’ personal autonomy rights protected? The answers to these questions will define both the power of the state to intrude into the private sphere and the quality of personal autonomy. What does privacy mean in the brave new world for the United States? How has the jurisprudence for law enforcement on the Fourth Amendment been shaped by the war on drugs?²³ One well-known and respected federal appellate judge, former Chief Judge of the First Circuit, Juan R. Torruella, noted over ten years ago in a celebrated article on the War on Drugs how prosecuting the war was reforming the basic tents of the Fourth Amendment, in particular in the search and seizure areas.²⁴ He lamented how for the first time courts had allowed the issuance of search warrants in drug cases based on anonymous tips, jeopardized the attorney-client relationship through the forfeiture of fees, and permitted grand juries to inquire into the attorney-client relationship.²⁵ According to Judge Torruella, to have courts approve such approaches undermined principles of legality and due process.²⁶

In the most recent Fourth Amendment search and seizure case involving drugs (crack cocaine rocks and unlawful firearm possession) and “the manner of entry,” or the “knock-and-announce rule” for a private home, *Hudson v. Michigan*, the Supreme court in a 5-4 decision split over the historic understanding of the “ancient principles in our constitutional order” of what constitutes the train of events of an “entry” under a

²² In the case of drugs, the other approach is to understand the issue more as a public health issue than a law enforcement or military problem.

²³ Amendment IV reads as follows: 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. U.S. Const. amend. IV.

²⁴ Juan R. Torruella, *Commentary: One Judge’s Attempt at a Rational Discussion of the So-Called War on Drugs*, 6 B.U. PUB. INT. L.J. 1 (1996).

²⁵ *Id.* at 24 (footnotes omitted).

²⁶ *Id.*

lawful warrant.²⁷ The issue before the court was the appropriate remedy – should the exclusionary rule be invoked to suppress the evidence of the search and seizure when the knock-and-announce rule is violated?²⁸ The remedy to a Fourth Amendment violation is essential to the impact it will have on a law enforcement community.

The stipulated facts of *Hudson* were clear. When the police arrived to execute the warrant they waited perhaps “three to five” seconds rather than a “20-second” pause suggested by previous precedent, or a reasonable amount of time, before entering Booker T. Hudson Jr.’s unlocked residence.²⁹ The time delay affords the homeowner time to protect life, property, and dignity but it should not prevent the government from seizing the evidence described in the warrant.³⁰

Justice Scalia’s majority opinion denying the suppression remedy focused on the legality of the warrant, particularly when the evidence sought or taken was specifically described in the warrant.³¹ In weighing the social costs of excluding the evidence, Justice Scalia focused on the evolution of the law in the Fourth Amendment context, intriguingly highlighting the “extant deterrents” that have been in place since the outlawing of warrantless searches under *Week v. United States*³² and *Mapp v. Ohio*.³³ The majority opinion relied on the fact that injured litigants now have civil action remedies under 42 U.S. C. §1983 and *Bivens v. Six Unknown Federal Narcotics Agents*, for entry violations and that over the past half-century there has been increased professionalism of police forces including a new emphasis on internal police discipline.³⁴ In short, the remedy for the violation of the “knock-and-announce rule” in the words of Justice Kennedy’s concurring in part and concurring in judgment opinion was “not sufficiently related to the later discovery of the evidence to justify suppression.”³⁵

Justice Breyer, in an ironic dissent, traced the lineage of the “knock-and-announce rule” back to the 13th century citing *Wilson v. Arkansas*, 514 U.S. 927 (1995), as the key precedent where the Court held the rule was a “basic principle” that “was woven quickly into the fabric of early American law”³⁶ and that the Framers thought the “method of an of-

²⁷ 126 S. Ct. 2159 (2006).

²⁸ *Id.* at 2163.

²⁹ *Id.* at 2162.

³⁰ *Id.* at 2165.

³¹ *Id.*

³² 232 U.S. 383 (1914).

³³ 367 U.S. 643 (1971).

³⁴ 403 U.S. 388 (1971).

³⁵ See *Hudson*, 126 S. Ct. at 2170. Justice Kennedy refused to join the majority on its interpretation of other warrantless searches in *Segura v. U.S.*, 468 U.S. 796 (1984) and *New York v. Harris*, 495 U.S. 14 (1990).

³⁶ 514 U.S. 927, 932-33 (1995).

ficer's entry into a dwelling was among the factors to be considered in assessing the reasonableness of a search or seizure."³⁷ For Justice Breyer, the precedents are clear, and suppression of the evidence is required:

We have held that a court must "consider[r]" whether officers complied with the knock-and announce requirement "in assessing the reasonableness of a search or seizure." *Wilson*, see *Banks*. The Fourth Amendment insists that an unreasonable search or seizure is, constitutionally speaking, an illegal search or seizure. And ever since *Weeks* (in respect to federal prosecutions) and *Mapp* (in respect to state prosecutions), "the use of evidence secured through an illegal search and seizure" is "barred" in criminal trials. (full citations omitted)

For another thing, the driving legal purpose underlying the exclusionary rule, namely, the deterrence of unlawful government behavior, argues strongly for suppression. See *Elkins v. United States* (purpose of the exclusionary rule is "to deter—to compel respect for the constitutional guaranty . . . by removing the incentive to disregard it"). In *Weeks*, *Silverthorne*, and *Mapp*, the Court based its holdings requiring suppression of unlawfully obtained evidence upon the recognition that admission of that evidence would seriously undermine the Fourth Amendment's promise. All three cases recognized that failure to apply the exclusionary rule would make that promise a hollow one, see *Mapp*, supra, at 657, reducing it to "a form of words," *Silverthorne*, supra, at 392, "of no value" to those whom it seeks to protect, *Weeks*, supra, at 393. Indeed, this Court in *Mapp* held that the exclusionary rule applies to the States in large part due to its belief that alternative state mechanisms for enforcing the Fourth Amendment's guarantees had proved "worthless and futile."³⁸

As the divided court makes clear there are two paths emerging over the power, extent, and breadth of the Fourth Amendment and how the courts will enforce the process by which law enforcement execute warrants. Exclusion of evidence has always been a remedy that forces law enforcement to follow rules – it is yet to be tested how training and civil suits affect law enforcement behavior patterns.

³⁷ *Id.* at 934.

³⁸ *Hudson*, 126 S. Ct. at 2173-74.

But the issue is larger than just how the Fourth Amendment is interpreted to police the police. How U.S. Congress and the courts balance the challenges of privacy, national security, and the war on drugs, technology and the Fourth Amendment will define our concept of citizenship. This challenge is not solely an “American” challenge but ultimately a world challenge. The Club of Rome, a global think tank, has identified the critical global issues confronting the planet: environment, demography, development, values, governance, work in the future, the information society, new technologies, education, the new global society, and the world economic and financial order.³⁹ Technology and security have become intertwined issues. Some have characterized the new interconnected world situation as a “world problematique.”⁴⁰

In the same vein, in 2003 the World Summit on the Information Society (“WSIS”), a meeting endorsed by the United Nations General Assembly, published its “Declaration of Principles—Building the Information Society: A Global Challenge in the New Millennium,” stressing a common vision for the access to information and knowledge.⁴¹ The WSIS is calling for a “model of cooperation” for the Internet whereby control would become internationalized and nationalized. China, for example, monitors and censors web communications that use such terms as “liberty” or “Falun Gong.”⁴² The world has recognized the trilemma of balancing technology, security, and privacy, and there is a struggle taking place over who will control the “electronic superhighway – the private sector, governments or international institutions.” In the European Union the principles of data protection and state responsibilities are enshrined in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 for the protection of individuals with regard to the processing of personal data and on the free movement of such data.⁴³ In May 2006, for example, the European Court of Justice upheld

³⁹ See The Club of Rome, Global Issues, http://www.clubofrome.org/about/global_issues.php (last visited Dec 1, 2006).

⁴⁰ See William J. Drake *Collective Learning in the World Summit on the Information Society* 8 (Computer Professionals for Social Responsibility, Working Paper Series No. 2, 2005), available at <http://www.cpsr.org/pubs/workingpapers/2/Drakepdf>; see also The Club of Rome, World Problematique, http://www.clubofrome.org/about/world_problematique.php (last visited Dec 1, 2006).

⁴¹ G.A. Res. 56/183, U.N. Doc. A/RES/56/183 (Dec. 21, 2001); Int’l Telecomm. Union [ITU], *World Summit on the Information Society Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium*, at 6, Doc. WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003), available at <http://www.itu.int/wsis/docs/geneva/official/dop.html>.

⁴² Mark A. Shiffrin and Avi Silberschatz, OpEd., *Web of the Free*, N.Y. TIMES, Oct. 23, 2005, § 4, at A13.

⁴³ See The European Commission, Freedom, Security and Justice, http://europa.eu.int/comm/justice_home/fsj/privacy/ (last visited Dec. 1, 2006). For a statement of the state principles see Directive 95/46/EC particularly Ch. II Sec. I Art 6 at http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HD_NM_6.

a challenge by the European Parliament to an agreement between the U.S. and the European Commission and European Council providing for the transfer of extensive personal data on European air passengers to the authorities in the United States.⁴⁴ In 2004, the agreement gave American counterterrorism authorities access to thirty-four different types of information including names, passport details, credit card numbers, addresses and phone numbers of approximately 9.6 million passengers on all flights that originate from the twenty-five European Union member states.⁴⁵ The European Court gave the Commission a four-month grace period to negotiate a new treaty with the United States. More comparative work should be done to see how different states and emerging states are approaching the trilemma – information technology, security, and personal autonomy.

Europe has taken an aggressive approach to data protection, the key to personal autonomy. Yet, at the same time Great Britain, in its fight against Irish terrorism, created one of the most watched “public spaces” in western society as demonstrated by its investigation against the recent radical Islamic bombings.⁴⁶ For example, as catalogued by Jeffrey Rosen, Britain has helped lead the way in public camera surveillance. He noted in 2001 that “in 1994, 79 city centers had surveillance networks; by 1998, 440 city centers were wired. By the late 1990’s, as part of its Clinton center-left campaign to be tough on crime, Tony Blair’s New Labor government decided to support the cameras with vengeance. There are now so many cameras attached to so many different surveillance systems in the U.K. that people have stopped counting. According to one estimate, there are 2.5 million surveillance cameras in Britain, and in fact there may be far more.”⁴⁷ Today in London there are “at least 500,000 cameras in the city and one study showed that in a single day a person could expect to be filmed 300 times.”⁴⁸ The U.S. is beginning to take the same approach and install cameras in major cities at critical sites. As many have pointed out, eventually, with the right algorithm and imaging, the authorities will be able to pick you out of the data mine of stored images and your life patterns will be clear.

⁴⁴ See Nicola Clark, *European Court Bars Passing Passenger Data to U.S.*, INT’L HERALD TRIB., May 31, 2006, at 1, available at <http://www.iht.com/articles/2006/05/30/news/fly.php>.

⁴⁵ *Id.*

⁴⁶ Steve Stecklow, Jason Singer & Aaron O. Patrick, *Watch on the Thames: Surveillance Cameras Monitor Much of Daily Life in London, May Help to Identify Bombers*, WALL ST. J., July 8, 2005, at B1, available at http://online.wsj.com/public/article_print/SB113077340647880052-cKyZgAb0T3asU4UDFVNPWrOAqCY_20060708.html.

⁴⁷ Jeffrey Rosen, *A Watchful State* N.Y. TIMES, Oct. 7, 2001, § 6 (Magazine), at 38.

⁴⁸ Stecklow, Singer & Patrick, *supra* note 46, at B1.

In contrast to much of the world, on these issues of technology and privacy, Congress has traditionally taken an approach informed by our Fourth Amendment jurisprudence. Judicial oversight has been the “American Way,” as stipulated by Title III in the 1968 Omnibus Crime Control and Safe Streets Act (“Title III”), the Electronic Communications Privacy Act of 1986 (“ECPA”), and the hotly debated Communications Assistance for Law Enforcement Act of 1994 (“CALEA”).

According to the Title III record, since 1968 judges have authorized approximately 31,000 wiretaps, 10,750 by federal judges and 20,225 by state judges. Between 2001-2004 there were 6,001 Title III electronic surveillances, or in other words, 1/5 of the total number of wiretaps have taken place over these last four years.⁴⁹ The theory has been that independent judges should be required to review the offer of proof by law enforcement for probable cause before wiretaps, surveillance, and access to one’s home can be violated. This is part of the check and balance scheme so heralded in our constitutional system. The system assumes life-tenured, unelected federal judges to be the most impartial gate keepers as opposed to elected, for-term, state judges.

With the passage of the Patriot Act in 2001, controversy swirled around the sunset clauses: § 203 – the authority to share criminal investigative information; § 206 – the roving surveillance authority under the Foreign Surveillance Act; §§ 209, 212, 220 – access to wire and electronic communications; § 214, 215 – the pen register and trap and trace authority under FISA and access to business records under FISA (“Libraries Provision”); § 218 – the lowering of the “wall” that allegedly separated law enforcement and intelligence operations for certification requirements from “the purpose” to “a significant purpose”; and finally the issuance of “national security letters” under the sole discretion of the Attorney General.⁵⁰ More recently “warrantless wiretaps” for national security reasons have sparked intense public debate.⁵¹ The fear was that the traditional Fourth Amendment protections of probable cause were being eroded as more and more information, without appropriate judicial review, was being accessed, viewed, processed, and controlled by government authorities. Critics wailed that Congress had broken the sacred bond of Fourth Amendment protection with any new legislation as the

⁴⁹ See Electronic Privacy Information Center, Title III Electronic Surveillance 1968-2005, http://www.epic.org/privacy/wiretap/stats/wiretap_stats.html.

⁵⁰ The best description of the debates is contained in AM. BAR ASS’N STANDING COMM. ON LAW AND NAT’L SEC., PATRIOT DEBATES: EXPERTS DEBATE THE USA PATRIOT ACT (Stewart A. Baker & John Kavanagh eds., 2005).

⁵¹ See Larry Abramson, *Q&A: The NSA’s Domestic Eavesdropping Program*, NPR, May 17, 2006, <http://www.npr.org/templates/story/story.php?storyId=5187738> (last visited Feb. 10, 2007).

traditional distinction between “citizen” and “non-citizen” was being undermined.⁵²

Defenders argued that the new threats, the new technologies, and the new demands for security required us to stop tying our hands behind our backs and create new powers of cooperation among law enforcements, intelligence agencies, and foreign allies.⁵³ The technology offered a new opportunity to “connect the dots” in the name of national security.⁵⁴ The historic distinction between domestic and foreign was being eroded by technologies, markets, and collective actions such as the internet; therefore, a new paradigm of national defense was needed. Traditional distinctions in the law between “citizens” and “non-citizens,” although valid, required recalibration.

As more and more personal data was being stored by third parties, like Internet Service Providers (“ISP”s), given the reduced expectation of privacy for data held by third parties, would a warrant be required? For some, the answer had to be “tech-savvy courts”:

This isn't a technology problem; it's a legal problem. The courts need to recognize that in the information age, virtual privacy and physical privacy don't have the same boundaries. We should be able to control our own data, regardless of where it is stored. We should be able to make decisions about the security and privacy of that data and have legal recourse should companies fail to honor those decisions. And just as the Supreme Court eventually ruled that tapping a telephone was a Fourth Amendment search, requiring a warrant—even though it occurred at the phone company switching office—the Supreme Court must recognize that reading e-mail at an ISP is no different.⁵⁵

But will the courts understand technology and data storage with this Fourth Amendment view? Much of the information is controlled by private parties – banks, insurance companies, credit card businesses, telephone companies, and internet providers. In short, what is private and what is public? How does one establish the boundary? What is the appropriate “reasonable expectation of privacy” in this new world of elec-

⁵² See David Cole, *Enemy Aliens*, 54 STAN. L. REV. 953 (2002); see also David Cole, *Their Liberties, Our Security: Democracy and Double Standards*, 31 INT'L J. LEGAL INFO 290 (2003).

⁵³ See John Yoo, *THE POWER OF WAR AND PEACE: THE CONSTITUTION AND FOREIGN AFFAIRS AFTER 9/11* (University of Chicago Press, 2005).

⁵⁴ See Shane Harris, *Group Proposes System to “Connect the Dots” about Terrorist Attacks*, <http://www.govexec.com/dailyfed/1104/111804hl.htm> (last visited Feb. 7, 2007)

⁵⁵ See Bruce Schneier, *Digital Information Rights Need Tech-Savvy Courts* <http://www.schneier.com/essay-080.html> (last visited Feb. 7, 2007).

tronic connectivity and potential threat of catastrophic damage? In a world where unmanned aerial vehicles (“UAVS”) can circle the battlefield and project force, should UAVS be deployed domestically for law enforcement purposes?⁵⁶ Is any open space private anymore?

What constitutes appropriate intrusion without a warrant for investigative purposes? Historically the Supreme Court has been the critical institution that has defined the US expectation of privacy. A recent case that joined this issue of public domain and private protection was *Kyllo v. United States*.⁵⁷ The United States Department of the Interior suspected that Danny Kyllo was growing marijuana in his home, which was part of a triplex.⁵⁸ Given that indoor marijuana growth typically requires high-intensity lamps, federal agents used an Agema Thermovision 210 thermal imager to scan the triplex.⁵⁹ Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth – black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images.⁶⁰

Interestingly, the district court found that the Agema 210 “is a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house”; it “did not show any people or activity within the walls of the structure”; “[t]he device used cannot penetrate walls or windows to reveal conversations or human activities”; and “[n]o intimate details of the home were observed.”⁶¹ The district court upheld both the validity of the warrant and its denial of the motion to suppress.⁶² On appeal, the court held that Kyllo had not shown a subjective expectation of privacy because he did not attempt to conceal the heat escaping from his home, and even if he had, there was no objectively reasonable expectation of privacy because the imager, “did not expose any intimate details of Kyllo’s life,” only “amorphous ‘hot spots’ on the roof and exterior wall.”⁶³

The 5-4 Supreme Court decision, written by Justice Scalia and joined by Justices Souter, Thomas, Breyer, and Ginsburg, reasoned that the eye unaided by technology (although previously airplane viewings

⁵⁶ See Peter Bowes, *High Hopes for Drone in L.A. Skies*, <http://news.bbc.co.uk/2/hi/americas/5051142.stm> (last visited June 6, 2006).

⁵⁷ 533 U.S. 27 (2001).

⁵⁸ *Id.*

⁵⁹ *Id.*

⁶⁰ *Id.* at 30.

⁶¹ *Id.*

⁶² *Id.*

⁶³ *Id.* at 31.

were held to be legal under *California v. Ciraolo*,⁶⁴) was constitutional, but when “the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a “search” and is presumptively unreasonable without a warrant.”⁶⁵ For many defenders of the Fourth Amendment the tying of the decision to “general public use” undermined the basic principle of the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. Do our protections turn on the issue of general availability and common use?

The dissent, written by Justice Stevens and joined by the Chief Justice Rehnquist, Justice O’Connor, and Justice Kennedy, turned on a constitutional distinction between “through-the-wall surveillance” where the observer or listener has direct access to information in a private area, and the thought processes used to draw inferences from information in the public space.⁶⁶

For the dissenters, the majority’s rule deals with direct observations of the inside of the home. However the case involved observations of the exterior of the home. According to the dissenters, “the supposedly “bright-line” rule the Court has created in response to its concerns about future technological developments is unnecessary, unwise, and inconsistent with the Fourth Amendment.”⁶⁷

What is appropriately in the public domain and what is private? In *Illinois v. Caballes*, the Court further reduced the concept of private space.⁶⁸ Justice Stevens, who authored the dissent in *Kyllo* wrote the opinion in *Caballes*, a 6-2 decision (one Justice was recused) upholding the sentence of a driver who had been stopped for speeding and was found to have illegal drugs in his possession.⁶⁹ While being detained for speeding, a dog sniffed the vehicle and the police found \$250,000 worth of marijuana in the truck.⁷⁰ Caballes claimed that using a “canine sniff” in the absence of a reasonable suspicion of illegal activity violated his Fourth Amendment right against unreasonable search.⁷¹

The Illinois Supreme Court reversed the lower trial court, stating that “specific and articulable facts” are necessary to justify the use of a drug-sniffing dog.⁷² For the United States Supreme Court majority, how-

⁶⁴ 476 U.S. 207 (1986).

⁶⁵ *Kyllo* 533 U.S. at 40.

⁶⁶ *Id.* at 41.

⁶⁷ *Id.* at 41.

⁶⁸ 543 U.S. 405 (2005).

⁶⁹ *Id.* at 406-407.

⁷⁰ *Id.*

⁷¹ *Id.*

⁷² *People v. Caballes*, 802 N. E. 2d 202, 205 (2003).

ever, “[a] dog sniff conducted during a concededly lawful traffic stop that reveals no information other than the location of a substance that no individual has any right to possess does not violate the Fourth Amendment.”⁷³ The ten-minute stop was held to be reasonable. For the dissenters, Justices Ginsburg and Souter, the precedent meant *random, suspicionless, drug-sniffing dog sweeps of unoccupied vehicles in parking lots or garages and on curbsides would almost certainly be completely permissible under the Fourth Amendment.*⁷⁴

For some, after *Caballes* the concept of privacy in automobiles was almost completely gone; it took only about seventy-five years. Will future Supreme Courts see electronic data, technology, and information more as part of the home and requiring warrants, or will the expectation of privacy erode as more technology becomes part of the general public use? Are electronic search engines, spiders, and “smart algorithms” really just electronic dogs doing data mining under the Fourth Amendment?

From the history of the Fourth Amendment and warrants, one sees a trend that is not overly comforting. The courts, when confronted with threats that may strike at the very core of society, have not always reinforced the Fourth Amendment. Congress has often aided and abetted during these periods and become captured by the sweep of emotions. In the early part of the 20th century, the “Red Threat” and the Palmer Raids created such national fear that the courts restricted speech and punished dissenters. During the period of prohibition and the introduction of cars as modes of transportation, the Supreme Court crafted the right to search in “plain view” exception to the Fourth Amendment.

During World War II, the Japanese internment camps undermined the Fourth Amendment and the concept of “individualized” guilt. Subsequent generations have viewed these internments as “self-inflicted wounds” but placed within the context of the times.⁷⁵ In the “Red Scare” of the 1950’s, Congress under Senator McCarthy violated individual rights, and the courts by and large either stayed on the sidelines or were involved in enforcing death penalties, such as in the case of the Rosenbergs.⁷⁶ During the “War on Drugs,” and *Kyllo* notwithstanding, our concept of expectation of privacy has diminished significantly. Now the GWOT has placed new pressure on governmental authorities to

⁷³ *Caballes*, 543 U.S. at 410.

⁷⁴ *Id.* at 411.

⁷⁵ William H. Rehnquist, *ALL THE LAWS BUT ONE*, Chapter 15: World War II: Japanese Internment (Alfred A. Knopf, 1998).

⁷⁶ See Harvey Rishikof, *Rosenberg v. United States* (1953), in *THE PUBLIC DEBATE OVER CONTROVERSIAL SUPREME COURT DECISIONS*, (Melvin I. Urofsky, ed., 2006); Ethel & Julius Rosenberg, *Atomic Espionage*, in *100 AMERICANS MAKING CONSTITUTIONAL HISTORY* (Melvin I. Urofsky ed., 2004).

gather information to prevent attacks with potentially catastrophic dimensions – nuclear, biological, radiological, and chemical.

The prevention of such catastrophic events turns on timely and actionable information. Technology increasingly is giving us access to unprecedented information about each individual, as they become part of the global economy. It is becoming harder and harder to hide if you interact with the electronic cash nexus – credit cards, smart cards for car travel, and etc. The Department of Defense (“DoD”) proposed a total inform access program to tap these electronic data.⁷⁷ The Information Awareness Office of the Total Information Awareness program stated its mission was to “imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving total information awareness useful for preemption; national security warning; and national security decision making.”⁷⁸ The fear of “big brother” without judicial restraint, however, caused the program to be scuttled.

Technology may also change how we discover the “truth.” Brain pattern monitoring in the future may unlock the key to veracity. “Brain-fingerprinting of neuro-imaging,” given the right algorithms, is part of the promise of functional magnetic resonance imaging (“f.M.R.I.”) and truth telling.⁷⁹ Although this technique may be appropriate for foreign prisoners of war, under the current Geneva Conventions such techniques would be illegal.⁸⁰ Currently, such use of technology would be barred in the U.S. because U.S. citizens are under the Fifth Amendment’s protections against self-incrimination. Though the Supreme Court has allowed the taking of blood and DNA samples from defendants, it may have to determine in the future if such an imaging technique can be employed, just like a DNA or blood test. Needless to say Congress, to this point, has not been conspicuous by its silence on these topics.

For many the solution to this trilemma – information technology, security, and privacy – has been checks and counter-balances. How do we police this phenomenon? Do we continue to rely on Federal judges’ determination of warrants’ legality, or hire more inspector generals and empower them with greater authority? How about creating a civilian

⁷⁷ See Gene Healy, *Beware of Total Information Awareness*, CATO INSTITUTE (Jan. 20, 2003), <http://www.cato.org/dailys/01-20-03.html> (last visited Feb. 6, 2007).

⁷⁸ See “Total Information Awareness Resource Center,” <http://www.geocities.com/totalinformationawareness/> (last visited December 1, 2006).

⁷⁹ See Harvey Rishikof & Michael Schrage, *Technology vs. Torture*, Psychopharmaceuticals and Brain Imaging Could Make Prisoner Interrogation More humane. Should we use them?, SLATE, Aug. 18, 2004, <http://slate.msn.com/id/2105332>.

⁸⁰ See Geneva Convention III at <http://www.yale.edu/lawweb/avalon/lawofwar/geneva03.htm>.

advisory civil rights boards or requiring a tougher congressional oversight of the process? Are these measures enough?

The executive branch, composed of honest and patriotic citizens charged to defend the Republic, will be increasingly using these new technologies to “connect the dots” before incidents take place to prevent a disaster. The intelligence agencies have been reorganized into a new structure under the Director of National Intelligence. Only time will tell whether this latest reorganization will prove to be effective.

In this brave new world, what is our legitimate “expectation of privacy” when the key to protection is information? The Congress and courts are the shaper of the trilemma and the balancer to the executive branch, but will there be a Patriot Act II in the wake of another incident? How will the boundaries be drawn to contain the genie? Will the world community agree with our new rules?

Ironically, the more we grant court-approved and congressionally-authorized electronic access for security reasons, the more the demand will be for better encryption programs. The better the encryption programs to thwart the “smart sniffers,” the greater the need will be for physical entry either at message’s origin or message’s final destination. The cycle will continue. So what is the answer to the trilemma?

In the end, there is no easy answer. Indeed the “*genie is out of the bottle.*” Technology is creating new challenges for privacy and Congress must begin to address the issue in an open manner. More informed public debate and discussion of the risks and consequences of eroding the distinction between citizens and non-citizens, as viewed by the law, is required. Courts will address the issue in the time honored common law “case-by-case” manner, but the national security imperative will be a powerful weight on the scales of justice. If history is to be a predictor, without congressional guidance, the courts alone may not prove to be enough.

II. ARE THERE ANY PUBLIC POLICY LESSONS FROM THE WAR ON DRUGS?

In a recent essay on the *Lessons of the “War on Drugs for the “War” on Terrorism*, a group of social science researchers, Jonathan P. Caulkins, Mark A. R. Kleiman, and Peter Reuter, suggested six categories to compare the two “wars”: 1) crime control and investigation within the United States; 2) the use of prison to incapacitate offenders; 3) control efforts outside the United States and at the border; 4) financial investigation and control; 5) overall coordination of enforcement efforts; and

6) rhetoric, media, and communications issues.⁸¹ But the authors wisely cautioned that the two “wars” differed in fundamental ways: the scale of the activity to be suppressed; the structure of the organizations whose schemes one must try to foil; the motivations of their participants; the scale, structure, and direction of the related financial transactions; and the tolerance for failure.⁸² The authors further reasoned that “even if, as some argue, “the war on drugs has been a failure,” that would not imply the inevitable failure of the attempt to suppress terrorist actions. Nor would they recommend that we can simply adopt wholesale for counterterrorism successful strategies and tactics from the anti-drug effort.”⁸³ In short, the lessons identified in the drug wars, to quote the British, require nuance and subtlety.

In the area of crime control, for the terrorist struggle, there are no “consumers” as in the drug sense of those who create a demand for controlled substances. In drugs, as in terrorism, there has been little benefit in “hardening targets” e.g., redesigning streets or reinforcing cockpits.⁸⁴ Perpetrators have demonstrated that they can and will adapt to attempts to block the problem. Both counter strategies support “undercover operations” and both activities defend against penetration by using blood and clan ties as required prerequisites to the inner circles.⁸⁵ Drug distribution networks, however, are atomistic, not monolithic, with multiple paths from network to customer and can be in competition with each other.⁸⁶ This competition can be and has been exploited by law enforcement.

Terrorist groups in this sense are not in competition for the same market. For some, terrorist networks are more vertically and horizontally integrated in the manner of organized crime, like the La Cosa Nostra (“LCN”).⁸⁷ To fight LCN, the Justice Department under Robert F. Kennedy created the Organized Crime and Racketeering Section in the Criminal Division to work with city-based “strike forces.”⁸⁸ New legislation was pursued to give more weapons to the prosecution such as the Racketeer Influence and Corrupt Organization statute (“RICO”). The goal was

⁸¹ Jonathan P. Caulkins, Mark A. R. Kleiman & Peter Reuter, *Lessons of the “War” on Drugs for the “War” on Terrorism*, ESDP Discussion Paper ESDP-2002-05 John F. Kennedy School of Government, Harvard University, June 2002, available at http://bcsia.ksg.harvard.edu/BCSIA_content/documents/Lessons_of_the_War_on_Drugs_for_the_War_on_Terrorism.pdf.

⁸² *Id.*

⁸³ *Id.*

⁸⁴ *Id.*

⁸⁵ *Id.*

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

to create a capacity for a long struggle against the crime families.⁸⁹ In this period, the focus of the target was primarily domestic.

The new terrorist and drug cartels are more international in nature than historic crime families. Slowly, the government has reorganized itself and passed new legislation to fight radical Islamic groups with international connections. Part of the underside of globalization has been the “globalization” of crime and networks. Organizing the state for this brave new world had historically been incomplete and controversial.

Do the traditional crime justice system philosophies - deterrence, rehabilitation, and incarceration - work for terrorism? Have they worked against the drug cartels? In the world of drugs, personnel replacement, even with long-term incarceration, has been easy.⁹⁰ Part of the GWOT is to focus on “high value targets” that represent the key planning cells and spiritual leaders of the movement. These individuals are considered the “A” team who pose the biggest threat to the homeland.⁹¹ These individuals, in the analysis of Bruce Hoffmann, the noted terrorist analyst, understand the requirements for a successful terrorist operation and can put together the six key requirements: 1) knowledge of how to create damage, or ingenuity in developing new methods of doing so; 2) access to the requisite material means; 3) a supply of operatives willing to kill and perhaps to die; 4) the ability to raise money and move it around internationally; 5) an organization capable of putting these requisites together to carry out operations across borders; and 6) motivation, either intrinsic or extrinsic.⁹² In this “decapitation” thesis, taking out these “leaders” will go a far way in protecting the homeland. In the drug world, in contrast, studies estimate that a million Americans sell cocaine in a 12-month period.⁹³ The logic is that there are fewer highly skilled key personnel in terrorism than drugs, so replacement will be more difficult.

International control of “non-government organizations” with or without alleged state support outside of the United States has proven to be a thorny issue. Illegal activity on such a grand scale requires some degree of support or tolerance by a local government to be successful according to many in the arena of drugs and terrorism. How to respond to this inability to control a geographical area has become the challenge of the 21st century in the wake of the cold war. Example of this is when Panama was invaded 1989, and General Noreiga was removed and tried under drug charges in federal court. In Colombia, the U.S. government

⁸⁹ *Id.*

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² See *Re-thinking Terrorism in Light of a War on Terrorism: Hearing Before the Subcomm. on Terrorism and Homeland Sec., 107th Cong. 8-9 (2001)* (statement of Dr. Bruce Hoffmann, Vice President, External Affairs and Director, RAND Washington Office).

⁹³ Caulkins, Kleiman & Reuter, *supra* note 81, at 8.

has been supporting a long-term policy to aid the Colombian government in exercising control over the drug cartels with Plan Colombia.⁹⁴

The area of interdiction is perhaps the best way to demonstrate a significant difference between the two “wars.” As pointed out by social scientists, stopping 90 percent of the drugs entering the United States would be a spectacular success, but letting through even 10 percent of terrorists or materials for major terrorist acts could be a disaster.⁹⁵ What is in the end a tolerable degree of failure in the drug war is intolerable in the war on terrorism, if the homeland is involved.

In the arena of finance, a comparison of the magnitude of numbers involved in the two wars is best reflected in the fact that the estimated cost of financing the attack of 9/11 was approximately \$500,000, roughly nine minutes of revenue in the U.S. cocaine market.⁹⁶ Since 9/11, investigating money laundering and tracking illegal flows of money have increasingly risen to the top of the policy agenda.⁹⁷ The problem is that terrorist networks have retained the ability to transfer funds undetected particularly when the cost of some of the attacks are comparatively so cheap. The Hawala networks or the informal money transfer systems⁹⁸ still exist, and in the current high terrorist locations – Iraq and Afghanistan – improvised explosive devices are in strong supply cheaply. Given the low cost of terrorism – an individual willing to wear a bomb vest – stopping an attack by choking the financial resources appears a weak approach.

As noted by Caulkins, Kleiman, and Reuter the public policy lessons identified from the war on drugs are mixed.⁹⁹ In essence, the drug wars have limited lessons for the war on terrorism and the history of fighting drugs is a sobering story. The enforcement problem for the two wars or campaigns is very different. There are no “customers” for terrorists as in drugs, and the leadership for international terrorism may prove to be as interchangeable as drug cartel leaders. How deterrence and incapacitation will work against terrorism remains an open question. Border interdiction has proven to be a failure in the drug context and it is unclear how the government will be more successful against a deter-

⁹⁴ See Bill Weinberg, *Washington Votes for War in Colombia*, THE NATION, posted Oct. 19, 2004, at <http://www.thenation.com/doc/20041101/weinberg>.

⁹⁵ *Id.* at 10.

⁹⁶ *Id.* at 12.

⁹⁷ See Testimony of Stuart A. Levey, Under Secretary Terrorism and Financial Intelligence U.S. Department of the Treasury BEFORE THE HOUSE FINANCIAL SERVICES COMMITTEE, September 22, 2004 at <http://www.ustreas.gov/press/releases/js1940.htm>.

⁹⁸ See Leonides Buencamino & Sergei Gorbunov, *Informal Money Transfer Systems: Opportunities and Challenges for Development Finance*, U.N. Dep't of Econ. and Soc. Aff. Discussion Paper Series (Nov. 2002), U.N. Doc. ST/ESA/2002/DP/26, available at <http://www.un.org/esa/desa/papers/2002/esa02dp26.pdf>.

⁹⁹ Caulkins, Kleiman & Reuter, *supra* note 81, at 8.

mined terrorist.¹⁰⁰ The money needs for a terrorist are comparatively small. The ability to exploit the money laundering networks for terrorist acts has been demonstrated by the successful attacks in Spain and England. Perhaps the most sobering lesson of the war on drugs concerns the organization of government institutions.

III. IS THE INSTITUTIONAL SOLUTION REORGANIZATION? – DHS? DNI? MI5?

For many commentators the critical answer for both “wars” is centered on creating the right governmental organizational structure so that effective coordination can be achieved.¹⁰¹ First, from the vantage point of personal autonomy, it is critical to note that the U.S. has, and continues to treat the drug issue as a criminal matter as opposed to a public health issue as have a number of European states.¹⁰² The whole “legalization” of drugs movement, although growing due to the efforts of many participants of this conference, still has not carried the day. As pointed out by researchers, the drug war domestically involves “more than a score of federal agencies, as well as uncounted state and local agencies. At the federal level alone, there are significant efforts by the Bureau of Prisons, the Drug Enforcement Administration (“DEA”), Federal Bureau of Investigation (“FBI”), the Customs Service, the Coast Guard, the Defense Department, the Education Department, the Department of Veterans Affairs, and the Substance Abuse and Mental Health Services Administration; each of these nine agencies each spends more than a billion dollars a year on anti-drug efforts.”¹⁰³

To coordinate the war, the Office of National Drug Control Policy (“ONDCP”) was created in 1989 with an announced mission of giving coherence to U.S. anti-drug efforts. ONDCP has a number of resources: “a director with cabinet status has the central role in promulgating an official National Drug Control Strategy, and statutory authority to “certify” agency budgets as adequate to the needs of that strategy, as well as to propose mid-year reallocations of resources within and across agencies, and management of a performance indicator system.”¹⁰⁴ In effect, a drug czar was placed in charge.

¹⁰⁰ See generally Stephen E. Flynn, *Beyond Border Control*, FOREIGN AFFAIRS, NOV/DEC. 2000 (for an explanation of the troubles in policing the border).

¹⁰¹ See President Bush’s remarks at signing into law the Intelligence Reform and Terrorism Prevention Act at <http://www.whitehouse.gov/news/releases/2004/12/print/20041217-1.html>.

¹⁰² See Van Solinge & Tim Boekhout, *Dutch Drug Policy in a European Context*, Journal of Drug Issues, Summer 1999 available at http://findarticles.com/p/articles/mi_qa3733/is_199907/ai_n8851692.

¹⁰³ Caulkins, Kleiman & Reuter, *supra* note 81, at 14.

¹⁰⁴ *Id.* at 16.

In addition to the creation of the ONDCP or a drug czar, a dedicated federal agency was given a single mission to fight the war: the DEA. Prior to 9/11 there was no analogous enforcement or intelligence organization dedicated to counterterrorist operations. The DEA's budget was \$1.7 billion for fiscal year 2003; it has a staff of 9,200, half of whom are special agents (i.e., criminal investigators with arrest powers), and it has experienced recent growth.¹⁰⁵ Nevertheless, it represents only 18 percent of all federal domestic counterdrug enforcement efforts.¹⁰⁶

Sadly, even with these organizational changes, the researchers lament that "predictably" there have been coordination problems between the DEA and other law enforcement agencies; the ONDCP has not been able to exercise true control over the federal drug budget; the creation of a national policy has been hampered by individual agency "veto" power; and congressional "balkanization" of budgets by different appropriations committees has hampered coherence.¹⁰⁷

The only light is that "the single-purpose character of the DEA means, among other things, that drug enforcement will not be entirely neglected when some other problem dominates public attention. The constancy of DEA's attention to the drug problem contrasts with the rapid cutback in the Customs Service's counterdrug efforts as it shifted efforts to the counterterrorism mission after September 11."¹⁰⁸

In the GWOT, a similar story emerges on the domestic front. The Federal Bureau of Investigation in post-war America was the lead agency in the war against terrorism. After 1946 two critical documents shaped the FBI's mission and roles in the area of national security and counterterrorism: the Foreign Intelligence Surveillance Act ("FISA") (1978) and Executive Order 12333 (1981). In the wake of 9/11, Congress enacted the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terror*¹⁰⁹ ("USA Patriot Act"), fundamentally changing the "12333/FISA" world. This legal regime separated criminal and intelligence matters to protect the political autonomy of US citizens. But the FBI remained the lead agency in the domestic fight against terrorism. No separate domestic agency dedicated to combating terrorism, such as MI5 in England, was created.

The organizational and programmatic solutions to criticisms of the government's performance pre 9/11 have been radical, beginning with the creation of the Department Homeland Security and the transfer of

¹⁰⁵ *Id.*

¹⁰⁶ *Id.* at 17.

¹⁰⁷ *Id.*

¹⁰⁸ *Id.*

¹⁰⁹ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terror*, H.R. 3162, 107th Cong. (2001).

former FBI functions such as the National Infrastructure Protections Center (computer security) to the new Department of Homeland Security. In addition, the Bush Administration took action on 37 of 39 of the 9/11 Commission's recommendations that apply to the Executive Branch making 13 key institutional changes:

- 1) **Appointing the Director of National Intelligence.** President Bush signed into law the landmark Intelligence Reform and Terrorism Prevention Act of 2004, which overhauls the intelligence community, mandating a range of reforms and centralizing in one office key authorities. The Director of National Intelligence (DNI) serves as President Bush's principal intelligence advisor and the leader of the Intelligence Community. The first DNI, Ambassador John Negroponte, was confirmed by the Senate and sworn in this past April.
- 2) **Establishing the National Counterterrorism Center (NCTC).** The NCTC assists in analyzing and integrating foreign and domestic intelligence acquired from all U.S. government departments and agencies pertaining to the war on terrorism. The Center identifies, coordinates, and prioritizes the counterterrorism intelligence requirements of America's intelligence agencies and develops strategic operational plans for implementation. In July 2005, the Senate confirmed the President's nominee, Vice Admiral Scott Redd, to become the first Director of the NCTC.
- 3) **Establishing the Domestic Nuclear Detection Office (DNDO).** The DNDO, in the Department of Homeland Security, provides a single federal organization to develop and deploy a nuclear-detection system to thwart the importation of illegal nuclear or radiological materials.
- 4) **Appointing a Privacy and Civil Liberties Oversight Board.** The President has nominated the Chairman and Vice Chairman and appointed the other three members to serve on the Privacy and Civil Liberties Oversight Board, to further help ensure that privacy and civil rights are not eroded as we fight the War on Terror.
- 5) **Establishing the Terrorist Screening Center.** In order to consolidate terrorist watch lists and provide

around-the-clock operational support for Federal and other government law-enforcement personnel across the country and around the world, the Administration created the Terrorist Screening Center. The Center ensures that government investigators, screeners, and agents are working with the same unified, comprehensive set of information about terrorists.

- 6) **Transforming the FBI to Focus on Preventing Terrorism.** The President has led the effort to transform the FBI into an agency focused on preventing terrorist attacks through intelligence collection and other key efforts, while improving its ability to perform its traditional role as a world-class law-enforcement agency. (e.g. “The service within the service” combining the counterterrorism and counterintelligence divisions into one branch.)
- 7) **Strengthening Transportation Security Through Screening and Prevention.** Since 9/11 the Transportation Security Administration (TSA) has made significant advancements in aviation security, including the installation of hardened cockpit doors, a substantial increase in the number of Federal Air Marshals, the training and authorization of thousands of pilots to carry firearms in the cockpit, the 100 percent screening of all passengers and baggage, and the stationing of explosives-detection canine teams at each of the Nation’s largest. These initiatives have raised the bar in aviation security and shifted the threat.
- 8) **Improving Border Screening and Security Through the US-VISIT Entry-Exit System.** US-VISIT uses cutting-edge biometric technology to help ensure that our borders remain open to legitimate travelers but closed to terrorists. US-VISIT is in place at 115 airports, 14 seaports, and 50 land border crossings across the country. Since January 2004, more than 39 million visitors have been checked through US-VISIT.
- 9) **Establishing the National Targeting Center (NTC) to Screen All Imported Cargo.** DHS established the NTC to examine cargo and passengers destined for the United States to identify those

presenting the greatest threat. The NTC screens data on 100 percent of inbound shipping containers (9 million per year) to identify those posing a "high risk." CBP personnel examine 100 percent of high-risk containers.

- 10) **Expanding Shipping Security Through the Container Security Initiative (CSI).** The CSI is currently established in over 35 major international seaports to pre-screen shipping containers for illicit or dangerous materials before they are loaded on vessels bound for the United States.
- 11) **Developing Project BioShield to Increase Preparedness For a Chemical, Biological, Radiological, Or Nuclear Attack.** Project BioShield is a comprehensive effort that will ensure that resources (\$5.6 billion) are available to pay for "next-generation" medical countermeasures, expedite the conduct of NIH research and development on medical countermeasures based on the most promising recent scientific discoveries, and give FDA the ability to make promising treatments quickly available in emergency situations. Project BioShield will help protect Americans against a chemical, biological, radiological, or nuclear attack.
- 12) **Cracking Down on Terrorist Financing With Our International Partners.** Over 400 individuals and entities have been designated pursuant to Executive Order 13224, resulting in nearly \$150 million in frozen assets and millions more blocked in transit or seized at borders. We have built an international coalition that is applying more rigorous financial standards and controls to help prevent terrorists' use of the international financial system. Specifically, we have established with the Government of Saudi Arabia a Joint Task Force on Terrorism Finance that serves as a coordinating mechanism to cooperate on important terrorism-financing investigations.
- 13) **Increasing Cooperation and Reform Among International Partners At The Front Lines Of The War On Terror.** In Pakistan over the next five years, we will provide more than \$3 billion in security, economic, and development assistance to enhance counterterrorism capacity and promote

continued reform, including of the education system. In the last three years, the United States provided more than \$4.5 billion in reconstruction, economic, and security assistance programs to Afghanistan.¹¹⁰

In the wake of 9/11 the U.S. has reorganized, but the ultimate question still remains: will this reorganization improve coordination among the sixteen intelligence agencies involved in the GWOT? In the event of another 9/11 event will more reorganization be called for?

IV. SHOULD AMERICA HAVE AN MI5?

The Department of Homeland Security (“DHS”) has a Department for Information Analysis and Infrastructure Protection, the Coast Guard and intelligence units. DHS, as is to be expected of a fledging federal institution defining itself in the more robust and institutionalized intelligence community, has had a slow start due to senior-level resignations, lack of analysts, and insufficient resources.¹¹¹ The decision to keep the FBI and CIA as separate institutions with DHS as a “client” for information guaranteed that the new organization would have to struggle to establish an intelligence role. As DHS battles for identity and function, there will be continuing bureaucratic tussles over whether the department’s primary focus is on acting as a “B” team that reexamines all the intelligence assembled by the FBI and the CIA, as a point agency for tightening security on “main street,” or as primary liaison to the private sector in the critical infrastructure sectors outlined by the Marsh Commission on security.¹¹²

In Britain, MI5 acts as a domestic analytical and spy agency. Being debated as an alternative solution is an “American” MI5, or an agency dedicated to protect the U.S. from terrorism and espionage.¹¹³ This would entail restructuring the FBI, DHS, and Treasury and hiving off the

¹¹⁰ See Press Release, The White House, Office of the Press Secretary, Progress On The 9/11 Commission Recommendations and Key Institutional Developments and Accomplishments (Dec. 5, 2005), <http://www.whitehouse.gov/news/releases/2005/12/20051205-5.html>. As highlighted by the White House, these 13 changes reflect the key institutional reorganization accomplishments of the executive branch.

¹¹¹ John Mintz, *Infighting Cited at Homeland Security, Squabbles Blamed for Reducing Effectiveness*, WASH. POST, February 2, 2005 at A01 at <http://www.washingtonpost.com/ac2/wp-dyn/A55552-2005Feb1?language=printer>.

¹¹² See John Mintz, *At Homeland Security, Doubts Arise Over Intelligence: United is Underpowered, Outmatched in Bureaucratic Struggles With Other Agencies, Critics Say*, WASH. POST, July 21, 2003, at A12; President’s Commission on Critical Infrastructure Protection, 1997; (“General Marsh Commission”).

¹¹³ See Fayza Elmostehi & Michael D. Vozzo, *Domestic Intelligence and National Security Reform Proposals*, <http://www.maxwell.syr.edu/campbell/Past%20Events/Papers/ISHS/ElmostehiVozzo.pdf>.

national security, counterterrorism and counterintelligence functions to combine all of the relevant analysts into one agency, as is currently the practice in Great Britain. In Britain, MI5 is under the Office of the Home Secretary and its agents have no arrest authority.¹¹⁴ The service is empowered with expansive investigative powers for domestic surveillance, intercepting all communications, eavesdropping, using informants and moles.¹¹⁵ Under this scenario, the FBI would function more like Scotland Yard and concentrate on traditional national crimes and organized crime violations. Presumably the new entity would also work closely with DoD assets to act as a clearinghouse for all of the relevant information from the thirteen major intelligence-gathering agencies.¹¹⁶ Needless to say, the resistance to the creation of MI5 comes not only from a philosophical resistance to the notion of a “domestic spy agency” with expanded powers, but also from all the existing intelligence bureaucracies who oppose the concept of losing such assets.¹¹⁷ The creation of DHS without significant intelligence powers reflects this dual resistance to an American MI5. Even with such an agency the issues of sharing information, analyzing information, and having constitutional and Congressional accountability still remain.

Given these constraints, a group of experienced former government officials suggested an interim MI5 approach that might be more bureaucratically acceptable to the intelligence community.¹¹⁸ Arguing for more information domestically on terrorist cells and the need for the integration of counterintelligence with counterterrorism that goes beyond a “case-file mentality,” the group called for the creation of a new and accountable agency within the FBI.¹¹⁹ Using the National Security Agency and the National Reconnaissance Office as models, it is envisioned that the new agency embedded within the FBI would have as its director a presidential appointee not from law-enforcement, be responsible to the directors of the DNI and CIA, be governed by Attorney General Guidelines, have its own independent personnel system for hiring, and have

¹¹⁴ Nigel West, *MI5 as a Model for an American Security Agency*, JOURNAL OF HOMELAND SECURITY, Aug. 2006, available at <http://www.homelandsecurity.org/newjournal/Commentary/displayCommentary2.asp?commentary=33>.

¹¹⁵ Don Van Natta Jr., *Threats and Responses: Antiterrorism*, N.Y. TIMES, July 26, 2003, at A8; see also MI5's Homepage, <http://www.mi5.gov.uk> (last visited Aug. 23, 2006).

¹¹⁶ Senator John Edwards, Homeland Security Address at the Brookings Institute (Dec. 18, 2002).

¹¹⁷ Todd Masse, *Domestic Intelligence in the United Kingdom: Applicability of the MI-5 Model to the United States*, CRS RL31920, May 19, 2003 at <http://www.fas.org/irp/crs/RL31920.pdf>.

¹¹⁸ *America Needs More Spies – Intelligence and security*, THE ECONOMIST, July 12, 2003, at 44 (The group of former officials includes from the FBI, Robert Bryant and Howard Shapiro; from the DoD, John Hamre; from DEA, John Lawn; and, from the CIA, John MacGaffin, and Jeffrey Smith).

¹¹⁹ *Id.*

direct oversight by the FISA court and Congress.¹²⁰ This approach was also recommended in 2005 by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (Robb-Silberman Commission) who suggested that the FBI needed a separate National Security Service within the FBI that included the Bureau's Counterintelligence and Counterterrorism Divisions, as well as the Directorate of Intelligence.¹²¹ The FBI responded and created the National Security Branch ("NSB") combining intelligence and counterterrorism. For some critics this was not enough.¹²²

The Intelligence Reform and Prevention of Terrorism Act ("Intelligence Reform Act"),¹²³ passed in December 2004, mandated the largest reorganization of the US intelligence community since the 1947 National Security Act and created a new Director of National Intelligence ("DNI"), instilled with expanded and overarching budgetary, acquisition, tasking, and personnel authorities to more effectively integrate the 15 members of the US Intelligence Community into a unified, cohesive, and coordinated enterprise.¹²⁴ The Intelligence Reform Act also created a National Counterterrorism Center ("NCTC") to serve as a true fusion center to collect, analyze, and disseminate all source information and intelligence – domestic and foreign – related to terrorism and counterterrorism.

Prior to the Intelligence Reform Act, the U.S. Intelligence Community was coordinated by a Director of Central Intelligence ("DCI"), with little statutory or budgetary authority over the community. The DCI also acted as the Director of the CIA and the President's principle advisor on all intelligence matters. To summarily state it, no DCI was ever able to successfully accomplish the task of coordinating the intelligence community. The coordination of the community was all but insurmountable, given the DCI's limited powers, and the enormous job of running the sprawling worldwide bureaucracy – the CIA.

Unlike a DCI, the DNI has no corresponding burden to manage an intelligence agency like the CIA. DNI only has to provide true overarching coordination and oversight among the intelligence community and to act as the President's principle intelligence advisor. In the year since his

¹²⁰ *Id.*

¹²¹ See THE COMM'N ON THE INTELLIGENCE CAPABILITIES OF THE UNITED STATES REGARDING WEAPONS OF MASS DESTRUCTION, REP. TO THE PRESIDENT OF THE UNITED STATES 451-52 (2005), available at http://www.wmd.gov/report/wmd_report.pdf.

¹²² See MICHAEL D'ARCY, MICHAEL O'HANLON, PETER ORSZAG, JEREMY SHAPIRO & JAMES STEINBERG, PROTECTING THE HOMELAND 2006/2007 (2006).

¹²³ The Intelligence Reform and Prevention of Terrorism Act, Pub. L. No. 08-458, Dec. 17, 2004 at http://www.nctc.gov/docs/p1108_458.pdf.

¹²⁴ Scott Jesse, *The Current Complexion of U.S. Counterterrorism* 43 (May 1, 2006) (unpublished paper, on file with author).

appointment as the first DNI in April of 2005, Ambassador John Negroponte has begun the effort to reshape and integrate the US Intelligence Community. He recently stated:

Our strategy focuses on protecting the nation today, making the nation safer tomorrow and building a stronger Intelligence Community right now. It requires aligning Intelligence Community members with these objectives so that we optimize the Community's total performance as opposed to optimizing its members' individual operations. We are in the process of remaking a loose confederation into a unified enterprise. This will take time—certainly more than a year—but with the right approach, it can be done.¹²⁵

As one can readily deduce from this solution, one of the continuing questions is: Who is in charge of integrating domestic law enforcement intelligence from the approximately 650,000 police officers, domestic federal agencies, and foreign national intelligence? Although the DNI is the titular head of the intelligence community, the director does not control approximately 80% of the intelligence budget, which is under the authority of the Secretary of Defense, and as a matter of law, the DNI director cannot operate domestically without severe legal constraints.¹²⁶ However, the DNI has coordination and budget authority over the FBI's new intelligence branch, the NSB.¹²⁷ Terrorist organizations that cut across domestic and foreign jurisdictions have created both legal and institutional problems. To resolve this dilemma, some have hoped that the new DNI is the answer for all intelligence issues.¹²⁸

No less a critic of the recent institutional reforms than Richard A. Posner, the respected appellate judge of the 7th Circuit, has called for a domestic intelligence agency separate from the FBI with no law enforcement responsibilities – a MIS or a DST – the French Direction de la Surveillance du Territoire.¹²⁹ Skeptical of the “service within a service” or NSB solution, Posner cites the classic criticisms of the FBI: the notorious computer failures; a chaotic and changing organizational structure

¹²⁵ See John D. Negroponte, Dir. of Nat'l Intelligence, Address Before the Nat'l Press Club: Intelligence Reform: Making It Happen, (Apr. 20, 2006).

¹²⁶ See Chapter 10, *Intelligence at Home: The FBI, Justice, and Homeland Security in the report of The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, (“The WMD Commission”), March 31, 2005 at <http://www.wmd.gov/report/>.

¹²⁷ D'ARCY, O'HANLON, ORSZAG, SHAPIRO & STEINBERG, *supra* note 122, at 32.

¹²⁸ WILLIAM E. ODOM, *FIXING INTELLIGENCE: FOR A MORE SECURE AMERICA* (1st ed. 2003).

¹²⁹ RICHARD A. POSNER, *UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM* 88 (2006).

(five alone since 1998); a retrospective criminal mindset of punishment not prevention; its geographical decentralization, the personnel department's resistance to support intelligence for career advancement; the turf conscious in-fighting against the CIA and now DNI; the lack of training for intelligence analysts; the specific problems of the Virtual Case File project; the fractured reporting structure of the head of the NSB to the FBI director, deputy director, Attorney General, and DNI; the split loyalties of the FBI director to criminal and intelligence matters; the advantage of a fresh start over reform within; and, finally the need to reform the "culture" of the law enforcement mind-set.¹³⁰

Recognizing the counter arguments that FBI-NSB should be given a chance to succeed, Posner is adamant that the FBI's "heavy hand" and culture will not change from within.¹³¹ He deplores the forty-six days on average the FBI needs for an application to the Foreign Intelligence Surveillance Court and is disparaging of the role the FBI has played in the Joint (federal-state-local) Terrorism Task Forces. Posner believes that specialization in international terrorism, as opposed to having jurisdiction for domestic attacks by the Animal Liberation Front, will provide the needed focus.¹³² In an ironic twist, Posner rejects the argument that keeping the FBI as the dominant domestic intelligence service will protect our civil liberties the best.¹³³ The FBI, due to the discipline of collecting and keeping evidence for criminal matters, has institutionalized our Fourth Amendment protections, and cannot treat material for intelligence purposes alone. This results in more risk for the homeland. The trilemma, however, continues whether we have an independent domestic intelligence service or not. How do we square the triangle?

CONCLUSION: SOVEREIGNTY AND CHOICE

The "long wars of political order" are not just for emerging democracies. Sovereignty lies at the heart of what constitutes a political regime, and a political regime is defined by how it protects its citizen's autonomy and choices. To Moisés Naím, however, "sovereignty is one of the thorniest issues of our times."¹³⁴ Conspicuously absent from the list of key institutional reorganization accomplishments are the changes taking place in the U.S. military and its new role in the struggle against terrorism and drugs. In the War on Drugs, the U.S. military plays an increasingly important role abroad as reflected in its participation in

¹³⁰ See *id.* at 87-109.

¹³¹ *Id.* at 111.

¹³² *Id.* at 114.

¹³³ *Id.* at 116-17.

¹³⁴ MOISÉS NAÍM, *ILLCIT: HOW SMUGGLERS, TRAFFICKERS, AND COPYCATS ARE HEJACKING THE GLOBAL ECONOMY* 274 (2006).

“Plan Colombia.” In 2000 the U.S. military began to train Colombia counternarcotics units, and subsequently the military in counterinsurgency against the Revolutionary Armed Forces of Colombia (“FARC”), the National Liberation Army (“ELN”), and the United Self Defense Forces of Columbia (“AUC”).¹³⁵ All three organizations allegedly fund their activities through drug revenues and are designated by the U.S. State Department as foreign terrorist organizations.¹³⁶ The narco-terrorist fusion has haunted Colombian politics for decades, and the civil war that is being waged is a test case for political order in the region. Counterinsurgency and counterintelligence continue to be the keys for the elected Colombian government. In the most recent election in May 2006, President Alvaro Uribe, for the first time in more than a century, was reelected as an incumbent president.¹³⁷ The previous president to do so was President Rafael Nunez in 1892. To protect the election process, approximately 220,000 troops guarded polling stations and other sensitive areas. As part of President Uribe’s “democratic security” agenda, he increased the number of troops and police on the streets by 25% and doubled military spending by obtaining financial backing from the U.S.¹³⁸ Under Plan Colombia, Uribe secured almost \$4 billion from the United States.¹³⁹ Since 2002 about 30,000 of the paramilitary group AUC have returned weapons under an amnesty agreement.¹⁴⁰ Moreover, approximately fifty-five politically motivated killings and kidnappings were recorded for the period of May 2005 to May 2006 – an 81% reduction from the prior elections in 2002, when the FARC kidnapped the candidate Ingrid Betancourt, who still remains captive.¹⁴¹ During this political process, Colombia remains the world’s largest producer of cocaine. While the rest of South America tilts left in Bolivia, Venezuela, Brazil, Argentina, Uruguay, and Chile – Colombia has voted for political order and a continued fight against cocaine. It remains a bloody and deadly unstable combination.

The War on Drugs is a choice that our legislature has made to restrain the private options of our citizens. Not all states and citizens have made the same choices. To some we have entered a period of “nanny-state paradigms” whereby the state plays the role of the parent prohibit-

¹³⁵ ANDREW FEICKERT, U.S. MILITARY OPERATIONS IN THE GLOBAL WAR ON TERRORISM: AFGHANISTAN, AFRICA, THE PHILIPPINES AND COLOMBIA 16-17 (2005), available at <http://www.fas.org/man/crs/RL32758.pdf>.

¹³⁶ *Id.* at 17.

¹³⁷ *Colombians Keep Uribe in Power in Landslide: U.S. Ally Has Led Fight vs. Rebels*, WASH. POST, May 29, 2006, at A17.

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.*

ing bad products.¹⁴² In “The Devil’s Picnic,” Taras Grescoe traveled the world, trying food, drugs, and drinks that are illegal and prohibited by one state or another. For example he sampled ‘Absinthe Suisse’ in Switzerland, coca leaves in the Andes, criadillas (bulls’ testicles) in Madrid, hjemmebrent, (a type of local moonshine) in Norway, Epoisses, (a cheese made from raw milk, not pasteurized and banned in the United States for health reasons) in France, a \$65 dollar Cohiba Esplendido Cuban cigar (banned in the United States for political reasons) in Montreal, poppy seed crackers in Singapore, and finally investigated a state assisted suicide club for non-citizens in Switzerland dollars that use overdoses of pentobarbital sodium for approximately \$2-3,000 as the preferred method of demise. Grescoe notes that in the Andes people have been chewing coca as far back as 2500 B.C.; such use is deep in the Andes’ culture. Ironically, to Grescoe banning or prohibiting commodities that people crave has historically resulted in three consequences: what is forbidden becomes more potent, and due to nonregulation, more deadly; it artificially inflates prices and creates fortunes for criminal actors that can bankroll internecine wars; and, it creates self-perpetuating institutions or enforcement agencies that exist to remove that which it has an interest in maintaining.¹⁴³

The regime of personal prohibition can be stifling. In the words of C.S. Lewis, “Of all tyrannies, a tyranny sincerely exercised for the good of all its victims may be the most oppressive. It may be better to live under robber barons than under omnipotent moral busybodies.”¹⁴⁴ Moreover, for Lewis:

Theocracy is the worst of all governments. If we must have a tyrant, a robberbaron is far better than an inquisitor. The baron’s cruelty may sometimes sleep, his cupidity at some point be sated; and since he dimly knows he is going wrong he may possibly repent. But the inquisitor who mistakes his own cruelty and lust of power and fear for the voice of Heaven will torment us infinitely because he torments us with the approval of his own conscience and his better impulses appear to him as temptations.¹⁴⁵

¹⁴² TARAS GRESCOE, *THE DEVIL’S PICNIC: AROUND THE WORLD IN PURSUIT OF FORBIDDEN FRUIT* 51 (2005).

¹⁴³ *Id.* at 352.

¹⁴⁴ C.S. LEWIS, *The Humanitarian Theory of Punishment* (1949) reprinted in *GOD IN THE DOCK: ESSAYS ON THEOLOGY AND ETHICS* (Walter Hooper, ed.) (1970).

¹⁴⁵ C.S. LEWIS, *OF OTHER WORLDS: ESSAYS AND STORIES* 81 (Walter Hooper, ed.) (1966).

The intrusive state that controls with a moral certitude is the antithesis of the liberal state based on personal autonomy. In the attempt to control the private “harm”, the public “cure” becomes a private toxin. So what is to be done with the “twin wars” that are connected at times and yet fueled by different private motives and public political goals? For Naïm the problem, or paradox, is one of “Black Holes v. Bright Spots.”¹⁴⁶ As sovereignty erodes and it becomes harder to control borders, Black Holes, the ungoverned spaces, become breeding grounds for all forms of illicit commodities and provide succor for international terrorism. The Bright Spots of prosperity cannot build impenetrable fortifications since being connected to the world of commodities, goods, and people are the keys to brightness. The darker the Black Hole, the more desperate are the people to be tied to the Bright Spots and sell goods, minds, work, illicit materials and even their bodies to traffickers. The two trends create ever-widening price differentials for all things and, therefore, an even greater incentive to connect the two worlds – hence the paradox. As pointed out by Naïm, illicit trade is driven by high profits not low morals; it is a political phenomenon supported by corruption; it is intertwined with licit trade; and governments cannot solve the problem alone. Naïm proposes enhanced, developed, and deployed technology as an answer – radio frequency identification devices; chemical and biological product tags; biometrics; detection and security devices; surveillance and eavesdropping; data mining and software; more global positioning satellites; and, finally biotechnology for an anti-cocaine vaccine.¹⁴⁷

In a world of asymmetric power, terrorists will not follow the rules of the nation states or the laws of armed conflict. In the end, only political solutions will end major terrorists’ acts. A political order with international penetrating and expansive technology for counterintelligence purposes will come at the expense of privacy, personal autonomy, and sovereignty as borders and transportation become increasingly transparent. This new political order will be very different from the classic 19th century liberal state, which for the last 200 years has been the ideal model of personal autonomy. The modern trilemma, and how it is finally resolved will dictate the relation of information technology, security, and private autonomy. But the wars may still go on, nonetheless.

¹⁴⁶ NAÏM, *supra* note 134, at 263-65.

¹⁴⁷ *Id.* at 239-47.