

Running head: COUNTER TERRORISM

Counter Terrorism: US Counter Terrorism Unit

Counter Terrorism: US Counter Terrorism Unit

Introduction

When terrorist attacks were perpetuated against the United States, the government is faced with the dilemma of instituting stricter security measures and infringing on the basic civil liberties of the citizens in exchange for the prevention of another repeat of the incident. The authorities struggle to strike a balance between security concerns and basic rights of citizens. The United States government's response to the 9/11 crises could be thought of as a knee-jerk reaction to the events. The hastily legislated PATRIOT Act sailed through Congress with the least resistance. Within six weeks from the day of terror, the House voted 356-to-66 and the Senate 98-to-1 to pass the anti-terror bill (Chang, 2001, p.1).

The Patriot Act affected the provisions of the First and Fourth Amendment. With the subversion of the Foreign Intelligence Surveillance Act (FISA) to include domestic applications, the Patriot Act inadvertently rendered the Electronic Communications Privacy Act (ECPA) signed into law by President Reagan in 1986 in recognition of the emerging technological issues and the Privacy Act of 1974 moot (Hayden, Hendricks and Novik, 1990, p.68). In addition, Paye (2006) astutely observed that the enactment of the Patriot Act effectively circumvented the judicial control and legitimized what he termed as a "frontal attack on the rule of law." (p.29).

The Patriot Act eradicated the boundaries between police and intelligence work. The judicial checks and balance were markedly absent and the Act provided the Executive branch the unrestrained right to exercise its prerogatives ignoring the basic tenets of the Constitution. Suspected persons could not invoke the Fourth Amendment as defense. Furthermore, the administration's demand for more power to implement measures judged to be preemptive strategies has created the impression that the Act was in support of self-preserving agenda.

The Gestapo-like tactic was defended and justified as a retaliatory strategy of the US government to external acts of aggression. Assistant Attorney General Daniel J. Bryant turned the proposition of self-defense on the Fourth Amendment on its head by propounding that “[i]f the government's heightened interest in self-defense justifies the use of deadly force, then it certainly would also justify warrantless searches.” (Chang, 2001, p.2)

The arguments presented above would mitigate the circumstances for the US government to turn to extreme measures in order to prevent a repeat of the 9/11 tragedies. Moreover, inherent defects in official protocol when dealing with sensitive information sent terrorism experts back to the drawing board and came up with a more cohesive plan for counter-terrorism. Strengthening the counter-terrorism units in local and federal governments had proved to be challenging.

The Changing Landscape of Counterterrorism

Alvin Toffler (1990), in his book *Power Shift* indicated that the axis of power is shifting towards the entity that possesses more substantial knowledge. Information technology in this case is both a powerful medium and a vulnerable platform. Just as the terrorist and criminal elements have the capacity to harness technology to advance their nefarious intentions, so can law enforcement agencies engage with them using state-of-the-art systems. Information technology has leveled the playing field.

Two such technology-driven counterintelligence measures include Echelon and Carnivore. The United States and its allies used Echelon to intercept communications intelligence from suspected perpetrators. Echelon is a code for a series of computers with the ability to decode intercepted communications. The National Security Agency is responsible for coordinating and implementing the strategy in the United States. The system is capable of

intercepting all forms of electronic communications including “land-line and cellular telephone calls, satellite communications, electronic mail, facsimiles, and various forms of radio transmission” (Sloan, 2001,p.1467+).

The Federal Bureau of Investigation (FBI) primarily uses carnivore as countermeasures against cyber crimes. The intention was to protect the interests of the American public against unlawful use of cyberspace to perpetrate crimes. The main targets of the Carnivore are “terrorism, information warfare, child pornography, fraud (including white collar), and virus writing and distribution” (Durham, 2002, n.p.). The Carnivore is capable of filtering e-mails from suspected criminals and tracing the origins of these messages. It operates on two modes, the “pen” and “full”. The “pen” mode will only capture the addresses of the messages while the “full” mode can access the entire contents of the e-mails (Etzioni, 2004, p.59).

Serious allegations have been thrown at the intelligence community for using Echelon and Carnivore other than what they were intended for. Some perceived abuses include using Echelon to conduct unlawful activities such as economic espionage. Within the United States, there are laws that would regulate the use of such technology. It is a fact that when electronic surveillance is applied as an intelligence measure, the privacy of individuals are violated. The success of electronic surveillance in this case involves some violation of the law.

When the Patriot Act extended the jurisdiction of the FISA, many believed that this was the remedy for dated and incompatible statutes that would regulate emerging technologies. However, civil liberties proponents advocated that the FISA has overextended its limits and the power of the Executive branch was deemed overreaching. Therefore, the risk of violating the provisions of the Fourth Amendment and the privacy of American citizens are not improbable.

With the FISA in place, any suspected individuals may be subject to investigations or surveillance without the need for a court order (Henderson,2002,p.179+).

Holland (2005) recognized that the current laws concerning emerging technologies are quite unclear. Procedurally, law enforcers may obtain warrants to search suspected electronic emails under Title I content warrant, Title II stored communications order, Title III pen register order, or a FISA warrant, without violating the provisions of the Fourth Amendment. The Patriot Act in this case, through FISA, merely circumvented the bureaucratic system as a quick response to protect the interests of the citizens and immediate apprehension of suspected terrorists or criminals. Emerging technologies require swift action or evidences may be rendered obsolete because of the rapid developments in information technology. In Kerr's (2003) opinion, the Patriot Act merely updated current laws on electronic surveillance. The passage of the Act had opened the debate on electronic surveillance laws and brought to light much needed discussions to create a balance between privacy and security. The law on electronic surveillance should be a work in progress to keep up with the pace of the developments in information technology (p.673).

Post-9/11 Counterterrorism Initiatives

With the passage of the Patriot Act into law, it gave government agencies leeway to set forth agendas to deal with terrorist threats against the state. All federal and state agencies were engaged in the plan to implement a more cohesive and working counterterrorism initiatives. Particularly, reforms were focused on the Federal Bureau of Investigation for its failure to prevent the 9/11 attacks. The intelligence agency is the lead federal government organization responsible for domestic security. The serious security gaps on the domestic front prior to the 9/11 attacks were traced to the lack of coordinated efforts to mitigate external threats because the

bureau was already burdened with cases in the domestic front. HUMINT was not extensively explored and used as a tool. Too much bureaucracy also undermined the ability of the bureau to perform its role in providing domestic security detail. The field offices functioned autonomously and crossing jurisdictions proved to be difficult. Finally, information was highly decentralized and often, sensitive information was hardly shared among the international community because these were closely guarded and would affect the cases in their respective jurisdictions (Chalk and Rosenau, 2003, pp.5-6).

Several agencies identified the gaps as serious and need rectification. Most prominent was the General Accounting Office's assessment that the bureau had communication failure and essentially "hampered the sharing of time-sensitive information both within the bureau and across other intelligence agencies." (Chalk and Rosenau, 2003, p.7). With those shortcomings, the bureau undertook several changes internally to bridge the gap.

The bureau transferred key counterterrorism personnel to its central offices to beef up its counterterrorism unit. Second, the bureau organized "flying squads" responsible for coordinating national counterterrorism efforts and assist local agencies. The National Joint Terrorism Task Force (NJTTF) was organized to coordinate city-level Joint Terrorism Task Force (JTTF). The NJTTF is equipped with "24-7 Counterterrorism Watch List (CWT) and two sections of Document Exploitation and Communications Analysis Center" (Chalk and Rosenau, 2003, p.10). The bureau's personnel also underwent re-organization and FBI recruits would be trained in "the latest intelligence assessment and forecasting procedures." (p.10). Information technology was harnessed to provide support for the initiative. To make the bureau run more effectively, the bureau's leadership also underwent an overhaul to make them function more proactively (pp.10-11). Robert Mueller, former bureau chief created four new directorships that would take care of

“criminal investigations, counterterrorism and counterintelligence, law-enforcement services, and administration (Conley, 2006, p.321).

With the organization of the Department of Homeland Security’s Information Analysis and Infrastructure Protection Directorate (IAIP) that would serve as repository for all intelligence information gathered by different investigative agencies, the bureau and all other intelligence community would channel their raw information for processing for non-federal officials’ use so they could also create strategies to protect key infrastructure within their respective jurisdictions (Chalk and Rosenau, 2003, pp.12-13).

Through EO13354 enacted on August 2004, established the National Counterterrorism Center (NCTC).The center’s main functions include:

- (1) to serve as the primary organization for analyzing and integrating intelligence;
- (2) to conduct strategic planning for counterterrorism;
- (3) to assign operational responsibilities to lead agencies with counterterrorism activities;
- (4) to act as a repository for data; and
- (5) to ensure that agencies have appropriate access to intelligence (Conley, 2006, p.324).

The center would oversee the intelligence duties of the FBI, CIA and Department of Defense (p.324).

Funding Sources and Training Initiatives

Attorney General John Ashcroft, in a bid to reinforce the strength of the Federal Bureau of Investigation (FBI) as lead agency to initiate counterterrorism strategies ordered in November 2001 that 10 percent of the total budget or \$25 billion dollars be devoted to anti-terrorism (Conley, 2006, p.319). Federal budgeting saw unprecedented increase to subsidize the need for a

coordinated counterterrorism strategies. Between 2002 and 2006, there was an increased in budget allocations to 38 percent or \$38.2 billion devoted to counterterrorism initiatives (Conley, 2006, p.327). By 2006, a third of the Federal Bureau of Investigations budget was allocated to hiring new recruits and conduct counterterrorism investigations. The increase was from 9,340 cases in 2001 to 33,000 cases in 2004 (Conley, 2006, p.330).

In addition to funding sources, two key areas were also affected by counterterrorism initiatives. To make counterterrorism measures more effective, investments should be made in “human resources for intelligence gathering and analysis, and training.” (Riley *et al*, 2005, p.37). Since the 9/11 occurred, personnel devoted to counterterrorism tasks had increased to 50 percent particularly in LAPD. Most of these increases were not a result of new hirings but more of reshuffling of personnel within each department or division. While there were increased interests in the counterterrorism, many agencies reported that they did not augment personnel training (Riley *et al*, 2005, p.37). This situation could prove to be worrisome as many of the officers were trained in effective “evidence gathering to support investigation of crimes and, ultimately, prosecution of offenses.” (p.38) However, there appeared to be a gap in the intelligence training area. Riley *et al* (2005) observed that the lack of funding prevented local agencies from sending their counterterrorism team members to train. The authors’ study also revealed that there was a lack of “standardization in analytical training across local, state, and federal agencies.” (p.38)

US Policy Changes in Post 9/11 Counterterrorism Milieu

The backbone of the policy changes of the United States concerning counterterrorism measures is the invocation of emergency powers by the Executive branch. What should have been a temporary state of emergency had evolved into a state of permanent exception. The reauthorization of the Patriot Act had revealed the true intentions of this administration. Article

212 authorized disclosure of communication, information and Internet accesses to the government without the benefit of a judicial courts accession to the act. Article 214 sanctioned the government to eavesdrop on suspected individuals without a warrant. Formerly, the police had to prove to the courts that there were mitigating circumstances that would justify such act. Under the reauthorization, the right to privacy was eroded and due process clearly ignored. Finally, Article 218 permitted authorities to conduct search and seizure on suspected individuals without cause. This law tolerated discrete searches on suspected individual's homes or places of work merely on the hint of suspicion.

The September 11 attacks also altered the foreign policy position of the United States. President Bush in his 2002 State of the Nation address articulated that "preemption and preeminence" was preferable to reliance on military presence. The Bush administration rooted its new foreign policy on the historical context of democracy with Secretary of State Condoleeza Rice reiterating in 2005 that the "freedom" was the "only realistic path to security" and "lasting justice." (Owens and Dumbrell, 2006, p.240).

Comparing Carl Schmitt's Model of Emergency Rule to Post-9/11 State of Exception

Carl Schmitt's decisionism was deeply rooted in Hobbesian philosophy. Hence the expediency of a decision coming from the Reich president was a necessary feature in Schmitt's exception rule. In politics, the sovereign had the final say and his decision generally shaped the nature and direction of the laws of the land. Schmitt's political theory was not hampered by the divisive nature of liberal democracies where every law was subjected to debate and discourse before it could be enacted (Scheuermann, 2006, pp.68-69).

In the case of the Bush administration, the liberal society advocated a decisionist position that was contrary to the norms and standards of the country. Not only was the post 9/11 situation

in a state of exception, so did the normative rule. The Constitution took a subordinate position. But unlike Schmitt's model, the Bush administration acted more like the destroyer of the Constitution than its guardian.

Under no circumstances did Schmitt suggest that the emergency state be evolved into a more permanent construct. The Bush administration made it appear that the PATRIOT Act was legally acceptable by asking the legislative and judicial branches to confirm the law hastily. The overwhelming majority decision and its completion at such a short time would make one suspect that eradicating the normal procedures had undermined the legal and political integrity of the Constitution.

Contrary to the meaning of the term patriot, decisionist's aims were "either more mundane—basic security and the enforcement of order—or more divine, as with those decisionists who see sovereign power as the divine essence realized on earth." (Lazar, 2006, p.258) In a way, the Bush administration heeded Schmitt's admonitions regarding the separation of powers advocated by liberal democracies. The emergency powers vested on the executive branch had far reaching implications in excluding the two major branches of government from decision-making in a state of emergency. To expedite the necessary, preemptive anti-terrorism measures, the administration took a radical path to implement the new rules. Public hearings and consultative meetings were eliminated. The administration, to justify their moves, legitimized the PATRIOT Act in the guise of a Congressional concurrence to the law. The fictional surrealism of George Orwell's novel "1984" became a reality in contemporary American society. With the legitimate Patriot Act, the government assumed the omnipresent "big brother" that controlled the lives of the population. The blatant invasion of privacy and unrestricted access to information that were formerly protected by the Constitution only illustrated the extent of power that the

Executive branch had attained in the course of implementing anticipatory measures against perceived enemies of the state.

This maneuver concurred with Schmitt's proposition that the expedient measures would eventually be legitimized if they were transformed into laws. The mechanisms that the original authors of the American Constitution had placed as a deterrent to potential abuse of power were surreptitiously removed. The Patriot Act had circumvented what was considered sacred and inalienable. Texas Republican Congressman Ron Paul observed that "[p]ersonal privacy, the sine qua non of liberty, no longer exists in the United States... The Patriot Act has given unbelievable power to listen, read, and monitor all our transactions without a search warrant being issued after affirmation of probable cause."(Paul, 2003,p.12)

American Hegemony: Extending Beyond National Borders

There are various reasons why the United States is considered the most powerful and influential nation in the world. Tracing the history of the rise of the Americans to world prominence, the primary concern of the United States is to protect its interests. One argument comes from the fact that rogue nations do exist and there is a need to keep them in check. Hitler's ambition to dominate the world was halted when the nations allied to prevent that. Heading that alliance was the United States. Having been successful at defeating the regime of the Third Reich in effect restored international peace. In order to suppress oppressive dictatorship and megalomaniac tendencies, the United States has to achieve military dominance. After the Cold War, American counterpart in the bipolar global politics showed signs of decline. It was in the 1990's that the United State's global power - military, economic, technological, cultural, and political (Ikenberry, 2003,p.2) proved to be a formidable combination and remained unmatched to this day. The balance of power has shifted and evolved into a unipolar paradigm.

The United States also should expect resistance from other powerful nations like Russia, China, Germany, France, Britain and Japan (Ikenberry, 2003, p.3).

The democratic ideals that have long been embraced by the Americans would benefit nations that are deemed weaker and prone to being prey to stronger, oppressive regimes. Buckner (2006) argued that:

The world is a far better place for having the United States as its lone Superpower. A world in which the strongest nation has in its Constitution a clause that prevents dictatorships, and leaves the ultimate power of the vote in the hands of its citizens is a world that carries the long-term hope of peace and stability.”

From a civilian point of view, Buckner (2006) further contended that the world is a better place with the United States overseeing the peace. The United States’ huge arsenal of arms and its principles regarding democracy and freedom protects that world from power hungry despots.

On the negative aspect, a scenario loomed darkly to extend to other countries, as many of the people subjected to surveillance were non-citizens. The Guantanamo Bay provided a milieu where the United States extended its contentious argument of exceptions. In a White House Statement, the detainees of the facility were not subject to the Article four of the Geneva Conventions because the prisoners did not conform to the criteria established for POW’s. The government further argued that they violated no treaty because Al Qaeda members imprisoned in Guantanamo “[were] not covered by the Geneva Convention, and [were] not entitled to POW status under the treaty.”(James S.Brady Briefing Room, 2003) Johns (2005) posited that the Schmitt’s proposition on decisions under exception rules cannot be “subsumed by existing norms.”(p.619) It was in effect in the facility. The procedures within the facility worked outside the extenuating covenants of the American Constitution and International treaties.

Conclusion

In the interest of providing security to the American citizens, the government may have encroached on some provisions guaranteeing the rights of every citizen. However, one must also recognize that current laws to counter terrorist activities are inadequate. With the advent of new technologies, the perpetrators are also abreast with the developments and have the intention to use any means to promote their self-interests. The government likewise will use every available means to counter terrorist acts against the country and its citizens. Both opposing camps would inevitably infringe on the basic rights of American citizens.

It is difficult to judge whether the government's response to the 9/11 attacks yielded more positive than negative results. The counterterrorism initiatives have yet to prove its effectivity. Questions regarding infringements on civil liberties and the Rule of Law should be addressed. Finally, despite the improvements and progress made to provide more domestic security, there are still gaps that need to be addressed. Funding and training are only two of the most important factors that would need immediate attention.

References

- Buckner, C. (2006) *Should America seek to be the greatest?* Retrieved August 11, 2007 from:
<http://www.renewamerica.us/columns/buckner/060112>
- Chalk, P. and Rosenau, W. (2003). *Intelligence, police and counterterrorism: Assessing post 9/11 initiatives.* Retrieved August 10, 2007 from:
<http://www.rand.org/nsrd/terrpanel/additional/intelinputv2.pdf>
- Chang, N. (2001). *The USA PATRIOT Act: What's so patriotic about trampling on the Bill of Rights?* Retrieved August 10, 2007 from: http://www.ccr-ny.org/v2/reports/docs/USA_PATRIOT_ACT.pdf
- Conley, R.S. (2006). Reform, reorganization, and the renaissance of the managerial presidency: The impact of 9/11 on the executive establishment. *Politics & Policy*, 34(2); 304-342.
- Durham, G.S. (2002). Carnivore, the FBI's E-Mail surveillance system: devouring criminals, not privacy. *Federal Communications Law Journal*. 54(3).n.p.
- Etzioni, A. (2004). *How patriotic is the Patriot Act? Freedom versus security in the age of terrorism.* New York. Routledge.
- Hayden, T., Hendrick, E. and Novik, J.D.(1990). *Your right to privacy: A basic guide to legal rights in an information society.* Carbondale, IL., Southern Illinois University Press.
- Henderson, N.C. (2002). The Patriot Act's impact on the government's ability to conduct electronic surveillance of ongoing domestic communications. *Duke Law Journal*. 52 (1); 179+.
- Holland, C. (2005) NOTE: Neither big brother nor dead brother: The need for a new Fourth Amendment standard applying to emerging technologies. *Kentucky College of Law Kentucky Law Journal*, Retrieved August 10, 2007 from: <http://web.lexis->

nexis.com.libproxy.sdsu.edu/universe/doclist?_m=553b3853c5f5e8f0a86465393739aff4
&_startdoc=26&wchp=dGLbVzW-
zSkVA&_md5=b7c8ef363bc70487a3541942f5bcec0c

Ikenberry, C.J (2003) *Strategic reactions to American preeminence: Great power politics in the age of unipolarity*. Retrieved August 11, 2007 from:

http://www.dni.gov/nic/PDF_GIF_2020_Support/2003_11_24_papers/ikenberry_StrategicReactions.pdf

James S. Brady Briefing Room. (2003) *Statement by the Press Secretary on the Geneva Convention* Retrieved August 11,2007 from:

<http://www.whitehouse.gov/news/releases/2003/05/20030507-18.html>

Johns, F. (2005) Guantánamo Bay and the annihilation of the exception. The European Journal of International Law.16(4); 613–635.

Kerr, O.S. (2003). Internet surveillance law after the USA patriot act: The big brother that isn't. Northwestern University Law Review; 97 (2); 607-673.

Lazar, N.C. (2006) Must exceptionalism prove the rule? An angle on emergency government in the history of political thought, Politics & Society, 34 (2); 245-275.

Owens, J. and Dumbrell, J. (2006). Introduction: Politics and policy in America's "War" on terror. Politics & Policy, 34(2); 233-256.

Paul, R. (2003). Trading freedom for security: Drifting toward a police state. Mediterranean Quarterly ; p.6-24.

Paye, J.C. (2006). A permanent state of emergency. Monthly Review. 58 (6);29-37.

Riley, K.J. *et al* (2005). *State and local intelligence in the war on terrorism*. Sta.Monica, CA: RAND Corporation.

Scheuerman, W.E. (2006). Survey article: Emergency powers and the rule of law after 9/11. The Journal of Political Philosophy, 14(1); 61–84

Sloan, L.D. (2001). Echelon and the legal restraints on signals intelligence: A need for reevaluation. Duke Law Journal; 50 (5); 1467+.

Toffler, A. (1990). *Powershift: Knowledge, Wealth and Violence at the edge of the 21st century*. New York. Bantam Books.