

The NATIONAL STRATEGY FORUM REVIEW

An Online National Security Journal Published by the National Strategy Forum

Homeland Security Gone Global

By Eric S. Morse

American domestic security has improved in the decade since the September 11th terrorist attack. The federal and state governments have improved their ability to prepare, respond, and recover from security emergencies. These developments are laudable, providing the American public with a relatively stable decade. Nevertheless, past stability is no indicator of future success. The U.S. domestic security apparatus is faced with a number of new security trends. The following is an overview of emerging security trends and the contextual framework by which to consider policy solutions.

A singular theme running through these trends is that homeland security is no longer confined to the activities that take place within U.S. borders. Homeland security is susceptible to the vagaries of the international system and must be cognizant of the external pressures placed upon domestic security system. Homeland security has gone global, and policymakers must adjust accordingly to this context.

Emerging Homeland Security Trends

Cyber Warfare: U.S. cyber security received a big boost when U.S. Cyber Command was launched in May 2010. The institutional arrival of U.S. Cyber Command is a strong step towards mitigating the threat. However, challenges to cyber security are looming. Perhaps the biggest threat is the continuous probing of U.S. networks from foreign sources. Deterring foreign cyber warfare is a very tricky proposition. Current international cyber warfare laws are vaguely defined and poorly implemented. A cyber security strategy must look to issues beyond our border to achieve deterrence. Key foreign partners in such a regime would be China and Russia. A global deterrence¹ strategy would include coordinating international cooperation, creating an international standard for reciprocity in the event of an attack, and defining what is appropriate cyber behavior for state and non-state actors.² This is a daunting challenge for the

¹ Deterrence theory includes the following components: a shared interest; deterrent calculation; a denial measure; a penalty measure; credibility; assurance; fear; and a cost-benefit calculation. For details, see Will Goodman's "[Cyber Deterrence: Tougher in Theory than in Practice?](#)" *Strategic Studies Quarterly*, Fall 2010.

² For an in-depth discussion of cyber deterrence strategy, see *NSFR Blog*: [Research Report William Goodman's "Cyber Deterrence: Tougher in Theory Than in Practice?";](#) and [A Strategy For Deterring Cyber Attacks.](#)

next decade. As governments seek to secure their complex networks from cyber warfare and cyber terrorism threats, they will find that international cooperation is vital for achieving success.

No More Secrets: The U.S. has entered an era where international, national, and personal secrets are no longer assumed to be safe. WikiLeaks, the General McChrystal scandal, corporate espionage, private disclosures on Facebook, juicy media news reports, and cyber security are all examples of information exposure with negative consequences. As an open, interconnected society, the U.S. thrives off of its transparency and freedom. However, such openness poses a provocative question: Is there anything that can truly be kept secret?³ Information is threatened from both interior sources (be it company employees, government officials, or a neighbor next door) and exterior sources (such as non-state and state actors, and corporate espionage). The consequences of exposed secrets can be devastating. Protecting secrets has a cost, as does losing control of secrets. The government and private sectors must develop strategies and policies that address a world in which there may be no more precious, enduring secrets. Determining which secrets, if any, are worth keeping is difficult. A balance must be found between protecting vital national security secrets and adjusting to a world that is becoming open source.

Biological Threats: The U.S. has been fortunate to have avoided forms of biological terror or widespread pandemic disasters. It was only a year ago that the H1N1 Swine Flu virus swept across the world, only to be more benign than originally expected. The question is are we more prepared to face next year's or next decade's biological outbreak? In addition, are we prepared for the possibility of biological, chemical or radioactive terror attacks?⁴ The domestic security trends indicate that defense gaps remain.⁵ Preparation should be viewed as a health insurance policy: one day you are bound to get sick and insurance prevents the costs from being overwhelming. In the early 1900s, the Spanish Flu killed 50-100 million people worldwide, with up to 500 million infected. Al Qaeda is pursuing the biological and radioactive means to carry out attacks. A prudent strategy would be to carry sufficient insurance. Such insurance includes setting aside funds for biological countermeasures, encouraging the private market to develop and produce vaccines and other medical countermeasures, and improving the rapid response and reach of the Center for Disease Control and the Department of Health and Human Services. However, a civil defense strategy against biological threats is expensive. It may be worth exploring a global biological defense structure that links states in developing joint biological countermeasures to share development and implementation costs. Finally, individual citizens should be empowered to take responsibility for protecting their own health by becoming more informed of possible threats and being enabled to purchase their own biological countermeasures in advance, rather than waiting for the government to supply the necessary doses after an event.

³ For more information, see the conference report titled "[No More Secrets: National Security Strategies for a Transparent World](#)." The conference was sponsored by the American Bar Association Standing Committee on Law and National Security, the Office of National Counterintelligence Executive, and the National Strategy Forum.

⁴ <http://www.vancouversun.com/news/Qaida+brink+using+nuclear+bomb/4205104/story.html>

⁵ Eric S. Morse. "[Russian Roulette with Project BioShield](#)." *The National Strategy Forum Review Blog*. July 28, 2010.

Black Spots: Ungoverned spaces, or “black spots,” are an emerging national security threat that is largely ignored by the post-9/11 security system.⁶ These areas are typically defined by the following characteristics: near an international border; overseen by a weak or ineffective government; exhibit high levels of government corruption; near trade routes; inhabited by heterogeneous populations; and generally unattended by media sources. A number of international examples of such places are locations in Yemen, Somalia, Southern Italy, the Pakistan tribal regions, and areas in Afghanistan. Concurrently, the threat to domestic security is that black spots reside both within and proximate to the U.S. Border areas along the Mexican and Canadian borders provide porous routes for the infiltration of drugs, criminals, and terrorists. Domestic black spots could even be defined as seemingly peaceful suburbs where disaffected individuals are free to plot extremist attacks on U.S. soil. The UK is no stranger to homegrown terrorism, and the U.S. is currently experiencing its own homegrown terrorist trend.⁷ A new research methodology is being employed to define, identify, and track black spots both domestically and abroad. The U.S. security apparatus must continue to adapt to this trend and deploy the resources necessary to prevent chaos from emerging from these areas.

Principles for Guiding Domestic Security Policy

To adapt to these security threats, five principles serve as a guide for creating policies. First, there is an ongoing tension between civil liberties and threat reduction. Security policy must remain compatible with the civil liberty and open society principles established by the U.S. Constitution. Second, policies must be affordable.⁸ Third, homeland security must be proactive—not reactive—in nature; proactive security investments should target emerging trends before the fruition of a threat. Fourth, the American public must recognize the role of personal responsibility in preparing for security threats; relying solely upon government is not always the most efficient option. Fifth, domestic security strategy should seek greater efficiency through cooperative strategies with friends and allies.⁹ With sufficient foresight, flexibility, and global outreach, America can continue to keep its citizens safe and secure.

Eric S. Morse is the Managing Editor of the National Strategy Forum Review, and a Doctoral Candidate in Political Science at Loyola University Chicago.

⁶ Bartosz Hieronim Stanislawski. “[Mapping Global Insecurity.](#)” *The National Strategy Forum Review*, Fall 2010, Volume 19, Issue 4.

⁷ Janet Napolitano: “We face a threat environment where violent extremism is not defined or contained by international borders.” February 10, 2011. “Officials Spotlight Domestic Terrorism Threat.” *Wall Street Journal*.

⁸ Richard E. Friedman. “[Affordability and National Security.](#)” *The National Strategy Forum Review*. Summer 2010, Volume 19, Issue 3.

⁹ Richard E. Friedman and Eric S. Morse. “[Complementary Strategy.](#)” *The National Strategy Forum Review*. Winter 2009, Volume 19, Issue 1.