A Practical Introduction to HOMELAND SECURITY and EMERGENCY MANAGEMENT

From Home to Abroad

Bruce Oliver Newsome
Jack A. Jarmon

1

HOMELAND SECURITY DEFINITIONS AND STRUCTURE

In 2007, in response to protests for the removal of a statue at a Soviet-era war memorial in the capital city of Tallinn, Estonia suffered persistent cyber attacks. Government ministry websites were defaced and disabled as well as those of targeted political parties, news agencies, banks, and telecommunication companies. A minister of defense in this nation of 1.3 million charged that "one million computers" attacked his country.

Although there was no loss of life, the incident demonstrated the impact such an attack could have. The collapse of tightly networked infrastructure can paralyze a state and make it a helpless victim to a brand of ***machtpolitik*** that is prevailing in the post–Cold War arena of conflict.

Investigators tracked the assault back to Russia. Implicated in the attack was a shadowy organization known as the Russian Business Network. It is a known cybercrime organization reputed to have ties with the Russian government, which denies the allegation. Accusations persisted and concerns about issues of **collective security** were strongly voiced. However, as quickly the alarms sounded, they became muted due to a lack of verifiable attribution (determining the source of a threat or belligerent or harmful action). Adding to the indecision were voids of definition, precedent, framework for resolution, and any clear policy on an appropriate response. Officials offered assurances that such action would not be tolerated but struggled to say how. Despite the pronouncements, policymakers had little recourse.

The above example draws attention to the disorientation experienced by the legacy institutions and cultures since the end of the Cold War. The onset of the new conflict left policymakers and military planners to assess an unfamiliar battle terrain and to reimagine a future of new threats and the new institutions that

Learning Objectives and Outcomes

At the end of this chapter, you should be able to do the following:

- Define security, homeland security, national security, international security, and related domains
- Explain public safety, domestic security, and emergency management
- Explain the difference between homeland security and counterterrorism and intelligence
- Explain how security is described at different levels (international, national, state, local, etc.)
- Describe homeland security in law, popular culture, and practice, incorporating the Canadian primacy of "public safety" and the British primacy of "home affairs"

(Continued)

will have to be built to counter them. The security establishment created institutions and mechanisms to address the problems of an interstate system. Most of the security framework traces back to the time of World War II. During the period of the Cold War, countries across the earth generally fell within one of two orbits. The collapse of that order and the advancement in information/telecommunication technology created a more borderless environment. Taking advantage of the anonymity and ubiquity of the virtual world, new opportunities for criminal and terrorist activity arose and continue to expand. Some of these groups can be state sponsored and have the ability and jurisdictional immunity to wage new wars, resume old rivalries, and make convenient and fleeting alliances. Their groups take advantage of the dynamism of globalization by exploiting the lacunae in global governance and law enforcement as well as the complexities of attribution.

The events of the 2000s exposed a new field of conflict. A new web of international relations, issues of governance, the role of the state, and the organizing elements of politics and economics set a complicated context for security policy. The definitions of national security and threat acquired new meanings. The shift from ***national security*** to ***homeland security*** signals a break from the past. Adversaries are indistinct and enigmatic. The threats also include natural catastrophes and the overuse of and over-reliance on fragile infrastructures. The homeland security environment and modern technology move ahead of policy. The consequences of these historical times may mean, in addition to creating a homeland security framework of well-defined policies and clearly communicated missions, legitimate society will need to collaborate in nurturing an evolving security environment in a hyperconnected world, which is transforming at a pace never previously known.

In this chapter, we discuss the definitions of homeland security, how various domains implement policy, and the history and structures that have occurred as a result of both events and planning.

(Continued)

- Describe the reorganization of the national-security establishment as a result of the events of September 11, 2001
- Describe the creation of the Office of Homeland Security and its transition to a cabinet level department
- Describe the budgeting process as it is proposed by the executive office and moves through Congress
- Describe the Department of Homeland Security (DHS) organizationally, and review the lineup of mission responsibilities and stakeholders
- Describe the coordination effort by DHS with state and local authorities in the areas of intelligence gathering, law enforcement, and emergency management
- Describe the influence of weapon technology as it relates to the nature of warfare and homeland security
- Understand how geopolitics has changed since 9/11 and the end of the Cold War

WHAT IS SECURITY?

Security is the absence of risks. Thus, security can be conceptualized as the inverse of risk and any risk sources or associated causes, including threats, hazards, exposure, or vulnerability (Newsome, 2014, Chapter 2). *Security* as a term is often used in combination or interchangeably with *safety*, *defense*, *protection*, *invulnerability*, or *capacity*, but each is a separate concept, even though each has implications for the other. For instance, *safety* implies temporary sanctuary rather than real security, while *defense* implies resistance but does not guarantee security.

According to semantic analysts, *security* is “the state of being or feeling secure” (FrameNet, 2012b). The state of being *secure* means that we are “certain to remain safe and unthreatened”

COMPARATIVE PERSPECTIVES

BOX 1.1

Different Legal and Official Definitions of Security

NATO

The North Atlantic Treaty Organization (NATO) describes *security* as “the condition achieved when designated information, materiel, personnel, activities and installations are protected against espionage, sabotage, subversion, and terrorism, as well as against loss or unauthorized disclosure” (2008, p. 2-S-4). A *safe area* is “in peace support operations, a secure area in which NATO or NATO-led forces protect designated persons and/or property” (NATO, 2008, p. 2-S-1). The *defence area* is “the area extending from the forward edge of the battle area to its rear boundary. It is here that the decisive battle is fought” (NATO, 2008, p. 2-D-3). Also central to the NATO mission is the concept of *collective security*. It is the notion that each state within the alliance agrees to the concept that security of one concerns the security of all.

Cooperative Cyber Defence Center in Tallinn, Estonia

Source: NATO. Retrieved from http://www.nato.int/nato_static_fl2014/assets/pictures/2014_05.

United States

For the U.S. Department of Defense (DOD, 2010), *security* is “1. Measures taken by a military unit, activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness. 2. A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts of influences” (p. 419). The DOD dictionary does not define *safety*, *public safety*, *defense*, or *defense area*, but admits a *safe area* is “a designated area in hostile territory that offers the evader or escapee a reasonable chance of avoiding capture and of surviving until he or she can be evacuated” (p. 269). *Civil defense* is “all those activities and measures designed or undertaken to: a. minimize the effects upon the civilian population caused or which would be caused by an enemy attack on the United States; b. deal with the immediate emergency conditions that would be created by any such attack; and c. effectuate emergency repairs to, or the emergency restoration of, vital utilities and facilities destroyed or damaged by any such attack" (p. 44).

Canada

The Canadian government has no official definition of *security* but the *Policy on Government Security* (effective July 2009) defines *government security* as "the assurance that information, assets and services are protected against compromise and individuals are protected against workplace violence. The extent to which government can ensure its own security directly affects its ability to ensure the continued delivery of services that contribute to the health, safety, economic well-being and security of Canadians" (Canadian Treasury Board, 2012, n.p.).

Public Safety Canada's internal *Security Policy* includes an effective operational definition of security; "security implies a stable, relatively predictable environment in which an individual or group may pursue its objectives without disruption or harm, or without fear of disturbance or injury" (n.p.). The Canadian government defines *public safety* as "the protection of all citizens by implementing measures that safeguard national security, improve emergency management, combat crime, and promote community safety" (Canadian Translation Bureau, 2015, n.p.).

Britain

The U.K. Ministry of Defence (MOD, 2009) uses the term *security* "to describe the combination of human and national security" (p. 6). The Development, Concepts and Doctrine Center says,

> Defence and security are linked, but different, concepts. Defence primarily refers to states and alliances resisting physical attack by a third party. Defence is about the survival of the state and is not a discretionary activity. Security is a contested concept that can never be absolute. It is therefore, to some extent, discretionary. It implies freedom from threats to core values both for individuals and groups. The decline in the incidence of inter-state war and the emergence of transnational threats, especially in the developed world, has resulted in greater political emphasis being placed on security rather than defence. Moreover, security has gradually evolved from the concepts of national and international security to the idea of human security. (2010, p. 76)

(FrameNet, 2012a). For criminologists, "security is the outcome of managing risk in the face of a variety of harms . . . [or] freedom from danger, fear, or anxiety" (Gibbs Van Brunschot & Kennedy, 2008, p. 10). For the Humanitarian Practice Network (2010), *security* is "freedom from risk or harm resulting from violence or other intentional acts" while *safety* is "freedom from risk or harm as a result of unintentional acts (accidents, natural phenomenon, or illness)" (p. xviii).

SECURITY DOMAINS

Security crosses many domains. A student is most likely to study security in disciplines like public administration; criminology and policing (in courses or fields titled "crime and justice," "transnational crime," "public safety," "public security," "counterterrorism," and "homeland security"); health and medicine ("public health" and "health security"); economics, political economy, or development studies ("economic security"); political science and international studies ("national security," "international security," "peace and conflict," "war studies," and "peace studies"); and military or defense studies ("strategic studies," "security studies," "security management," "defense management," and "military science"). Some courses ("counterterrorism" or "homeland security") are so truly interdisciplinary that they could be taught in any of these disciplines.

Consequently, a mix of disciplines, fields, and subfields (some of them ambiguous or contested) touch upon or converge in the study of security. Many people fret about insecurity but have disciplinary biases or formative experiences that constrain their study of security. Security crosses domains that academic disciplines and professional careers have tended to separate in the past.

COMPARATIVE PERSPECTIVES

BOX 1.2

Security—A Multidisciplinary Study

Studying security is a multidisciplinary project. It is not possible to think about security without recognizing that boundaries between realms such as health, crime, and the environment, for example, are often blurred, both in theory and in practice. This means that we must draw on a number of different fields of study to make sense of how balancing risk leads to security (or insecurity). While the primary target of much of the work on security has been criminal justice agencies, particularly law enforcement, the issues raised in addressing hazards from health and natural disasters include public health officials, engineers, scientists, and others . . . Although we bring to the project our backgrounds in sociology and criminology, we maintain that security is a subject that has yet to be adequately covered by a specific discipline or in a satisfactory interdisciplinary fashion. Furthermore, concerns over security are never far from issues that pervade the public and private domains. While public-health officials might concern themselves with flu epidemics and other transmissible diseases, for example, the goal of keeping populations healthy is ultimately a national and, increasingly, a global security issue for a vulnerable segment of the population, it also secures the public-health system by alleviating it from having to deal with the expenditures incurred if such epidemics were to occur. (Gibbs Van Brunschot & Kennedy, 2008, pp. 17–18)

The higher domains that concern everybody from the international to the personal level are national security, homeland security, international security, and human security, as described in the sections below, each structured by the U.S., Canadian, and British interpretations.

Human Security

The United Nations and most governments and nongovernmental organizations now recognize **human security** (freedom from fear or want). In 1994, the U.N. Development Programme published its annual report (*Human Development*) with a reconceptualization of human security as freedom from fear or want across seven domains:

1. Economic security
2. Food security
3. Health security
4. Environmental security
5. Personal security
6. Community security
7. Political security (human rights)

In 2001, Japan initiated the International Commission on Human Security. In May 2003, it published *Human Security Now*, which asserted human freedoms from pervasive hazards such as pandemic diseases. In May 2004, the U.N. Office for the Coordination of Humanitarian Affairs (OCHA) created a Human Security Unit. It defines *human security* as a concept that "(i) . . . concentrates on the security of the individuals, their protection and empowerment; (ii) drawing attention to a multitude of threats that cut across different aspects of human life and thus highlighting the interface between security, development and human rights; and (iii) promoting a new integrated, coordinated and people-centered approach to advancing peace, security and development within and across nations" (U.N. Office for the Coordination of Humanitarian Affairs, 2009, pp. 6-7).

Human security grew as a valued concept particularly among those who work on international or global development and humanitarian affairs. It is now included in military doctrines for stabilization, counterinsurgency, and counterterrorism after excessive focus on homeland security and national security in the 2000s. For instance, in the context of counterterrorism, human security has been defined as "freedom from fear or want for individuals or populations in terms of physical, economic, political, cultural and other aspects of security/absence of threat" (Beyer, 2008, p. 63).

COMPARATIVE PERSPECTIVES

BOX 1.3

Human Security and British Military Stabilization Operations

Security has traditionally been understood as National Security, concerning itself with territorial integrity and the protection of the institutions and interests of the state from both internal and external threats. However, increasingly, the understanding of security has been broadened to include the notion of Human Security, which emphasizes the protection of individuals who seek safety and security in their daily lives. Human security encompasses freedom from fear of persecution, intimidation, reprisals, terrorism and other forms of systematic violence as well as freedom from want of immediate basic needs such as food, water, sanitation and shelter. Importantly, where the state lacks the ability to meet the human security needs of the population individuals tend to transfer loyalty to any group that promises safety and protection, including irregular actors. Of note:

- There are obvious overlaps between national and human security. For example, the presence and activities of violent groups both exacerbates the fragility of the state and undermines the safety and security of the people.
- A stable state must protect the most basic survival needs of both itself and its people. This includes the provision of human security for the population in addition to the control of territory, borders, key assets and sources of revenue.
- A stable state exists within a regional context. As such it may import or export instability across its borders. Security issues that are outside of a host nation's direct influence will require regional political engagement. (U.K. MOD, 2009, pp. 1–6)

International Security

Most American political scientists acknowledge a field called *international relations*. Canadian, British, Australian, and similar academies are more likely to separate international relations or international studies as a discipline in its own right, but the place of international relations within or without political science remains contested everywhere.

Some academics recognize a field or subfield called *international security*. The American Political Science Association recognizes *international security and arms control* as a section. However, for ethical and practical reasons, the study of international security is not universally acknowledged. This is why Richard Betts advocated a political scientific subfield called *international politico-military studies*, which implies parity with other subfields, such as international political economy (Betts, 1997).

In the 1980s and 1990s, increased recognition of globalization and transnationalism helped to drive attention toward international security, but use of the term *international security* has declined steadily since its peak in 1987, despite a small hump from 1999 to 2001, while uses of *homeland security*, *economic security*, and *human security* have increased commensurately (according to Google Ngram). Some advocates of *international security* use it to encompass military, economic, social, and environmental hazards (Buzan, 1991). The concept of international security has revived since the 2000s as it has encompassed other forms of security. In particular, the supremacy of homeland or national security has collapsed as people realized the international sources of and solutions to homeland or national risks.

Soldier Meeting Children

Source: Human Security Report Project (2011). Best of the Marine Corps, May 2006, Defense Visual Information Center/Photo by Expert Infantry on Flickr.

National Security

UNITED STATES The United States has institutionalized *national security* more than any other state, particularly since 1947 with the National Security Act, which established a National Security Council (NSC) and national security adviser to the executive. For DOD (2010), national security encompasses "both national defense and foreign relations of the United States" and is "provided by a military or defense advantage over any foreign nation or group of nations, a favorable foreign relations position, or a defense posture capable of successfully resisting hostile or destructive action from within or without, overt or covert" (p. 320).

Publicly stated, the function of national security and the responsibility of its establishment are to create and maintain a favorable environment for United States' national interests—in times of both war and peace (Jarmon, 2014). The term *American values* can be elusive. Former Secretary of State Dean Acheson defined the expression *American values* by asserting that it involved the fostering and preservation of "an environment in which free societies may exist and flourish" (Jordan, Taylor, Meese, & Nielsen, 2009, p. 233). The standards of freedom, however, are left open to another layer of interpretation. This objective to create and maintain a favorable environment for U.S. national interests, Andrew Bacevich (2008) argues, has given the U.S. national-security establishment justification for force projection—an approach that seems to clash semantically and conceptually with notion of defense and the namesake of the cabinet department charged with that responsibility.

After the investigations of the attack on the World Trade Center, the 9/11 Commission released its findings. Among them was the following observation: "As presently configured, the national-security institutions of the U.S. are still the institutions constructed to win the Cold War" (National Commission on Terrorist Attacks Upon the United States, 2002, p. 399). Many internationalists and foreigners consider national security an inaccurate and possibly xenophobic concept, especially given increasingly international and transnational threats. In practice, most Americans use *national security* and *international security* interchangeably or to describe the same domains whenever politically convenient while the newer term *homeland security* has supplanted *national security*.

The events of September 11, 2001, forced a reorganization of the national-security establishment and the creation of the Department of Homeland Security. The new post–Cold War era also forced American policymakers and planners to revisit their vision

COMPARATIVE PERSPECTIVES

BOX 1.4

Official U.S. Conceptualization of International Security

Senator John Kerry, speaking at the University of Virginia on February 20, 2013, days after his confirmation as U.S. Secretary of State . . .

> I came here purposefully to underscore that in today's global world, there is no longer anything foreign about foreign policy. More than ever before, the decisions that we make from the safety of our shores don't just ripple outward; they also create a current right here in America. How we conduct our foreign policy matters more than ever before to our everyday lives, to the opportunities of all those students I met standing outside, whatever year they are here, thinking about the future. It's important not just in terms of the threats that we face, but the products that we buy, the goods that we sell, and the opportunity that we provide for economic growth and vitality. It's not just about whether we'll be compelled to send our troops to another battle, but whether we'll be able to send our graduates into a thriving workforce. That's why I'm here today.
>
> I'm here because our lives as Americans are more intertwined than ever before with the lives of people in parts of the world that we may have never visited. In the global challenges of diplomacy, development, economic security, environmental security, you will feel our success or failure just as strongly as those people in those other countries that you'll never meet. For all that we have gained in the 21st Century, we have lost the luxury of just looking inward. Instead, we look out and we see a new field of competitors. I think it gives us much reason to hope. But it also gives us many more rivals determined to create jobs and opportunities for their own people, a voracious marketplace that sometimes forgets morality and values.
>
> I know that some of you and many across the country wish that globalization would just go away, or you wistfully remember easier times. But, my friends, no politician, no matter how powerful, can put this genie back in the bottle. So our challenge is to tame the worst impulses of globalization even as we harness its ability to spread information and possibility, to offer even the most remote place on Earth the same choices that have made us strong and free.

of U.S. national security. The Department of Defense concept of force projection morphed into a "pushing out of the borders" strategy in homeland security. Some see the transition as a new vision for the future; others regard it as a variation on an old theme. Regardless, the security establishment and its apparatus continued to adjust to an era of indistinct borders and enigmatic foes.

Table 1.1 The U.S. National-Security Establishment

President					
Secretary of State • Deputy ○ Operational Units		Secretary of Defense • Deputy ○ Operational Units			National Security Council/National Security Advisor • Vice President • Secretary of State • Secretary of Defense • Chairman, Joint Chiefs of Staff • Director of National Intelligence • Director, CIA
Global Affairs Counselor Political Affairs Economic, Business, and Agricultural Affairs	Management Arms Control and International Security Public Diplomacy—Public Affairs	Secretary of the Army Office of the Secretary of Defense	Secretary of the Navy Inspector General Unified Combat Commands	Secretary of the Air Force Joint Chiefs of Staff	Advisors and Staff Nonstatutory Members Invited Attendees

Source: Jarmon (2014).

CANADA In 2003, the Canadian government established a Minister and a Department of Public Safety and Emergency Preparedness (Public Safety Canada). Public Safety Canada (PSC), as legislated in 2005, is not defined by national or homeland security but is responsible for only domestic civilian authorities: the correctional service, parole board, firearms centre, border services, the federal police, and the security intelligence service.

In April 2004, the Canadian government released its first national-security policy (*Securing an Open Society*), which specified three core national-security interests:

1. Protecting Canada and the safety and security of Canadians at home and abroad
2. Ensuring Canada is not a base for threats to our allies
3. Contributing to international security (Canadian Privy Council Office, 2004, p. vii)

The national-security policy aimed at a more integrated security system and declared objectives in six key areas:

1. Intelligence
2. Emergency planning and management
3. Public-health emergencies
4. Transportation security
5. Border security
6. International security (Canadian Privy Council Office, 2004)

The resulting institutional changes included the establishment of a National Security Advisory Council, an advisory Cross-Cultural Roundtable on Security, and an Integrated Threat Assessment Center.

In 2006, Public Safety Canada and the Department of National Defence (DND) created the Canadian Safety & Security Program "to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism" (Public Safety Canada, 2014b, n.p.)—a scope more like American homeland security, although no department of Canada's government has any definition of homeland security.

The federal government still lacks a federal definition of either *security* or *national security*, although the Defence Terminology Standardization Board defines "national security" as "the condition achieved through the implementation of measures that ensure the defence and maintenance of the social, political and economic stability of a country" (Canadian Translation Bureau, 2015, n.p.). DND recognizes *national security* as counterterrorism, infrastructure security, cybersecurity, and public safety and security generally—but not civilian border security (which falls under national law enforcement, for which the leading responsibility is Public Safety Canada) or military defense of Canada's borders or foreign interests. The *Policy on Government Security* (effective July 2009) defines the *national interest* as "the defence and maintenance of the social, political, and economic stability of Canada" (Canadian Translation Bureau, 2015). Public Safety Canada supports the Prime Minister in all matters relating to public safety and **emergency management** not covered by another federal minister. Public Safety Canada has defined its mission to achieve "a safe and resilient Canada," to enhance "the safety and security of Canadians" (2014a, p. 1), and to provide "leadership and guidance to federal government institutions, including in the preparation, maintenance, and testing of emergency management plans" (2012, p. 1).

The National Security Program is a coordinating and advisory mechanism within the Public Safety Portfolio that, when appropriate, works with other Canadian government offices on matters relating to international threats and threats to the territory of Canada. The areas of concern specifically include the following:

Critical infrastructure

Cybersecurity

Counter terrorism

Listing and de-listing of terrorist entities

Foreign investment risk

Radicalization leading to violence

Proliferation of weapons of mass destruction

It coordinates, analyzes, and develops policies and implements processes related to the above issues as it also advises the government on the impact of such policies and courses of action on individual rights and legislation.

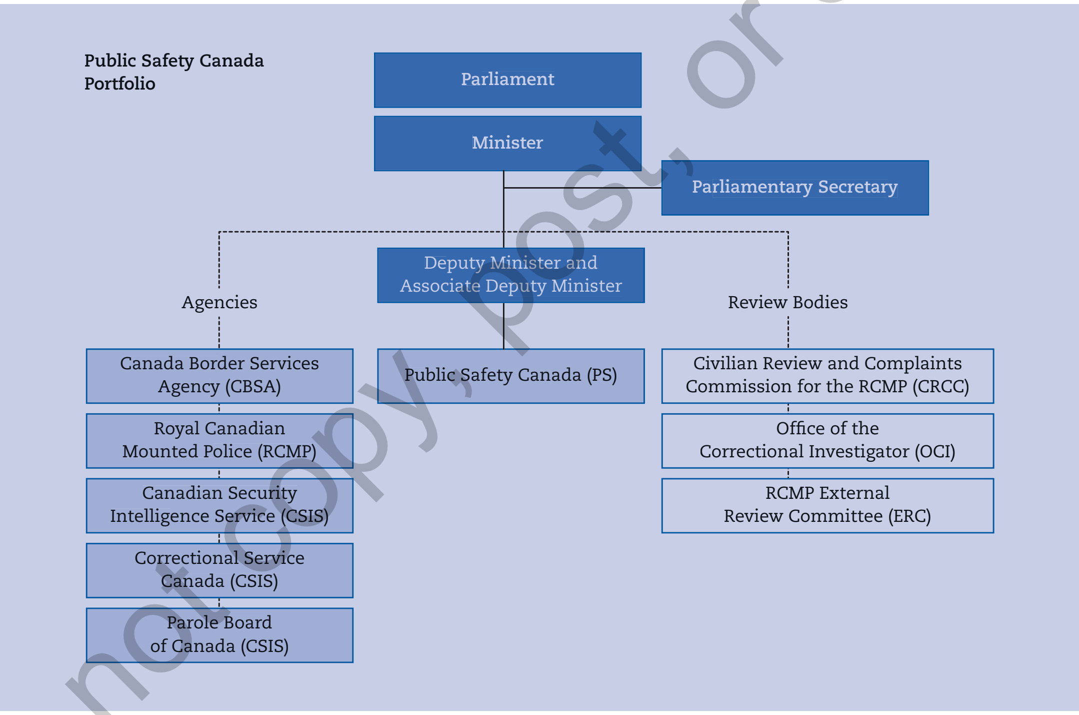
Table 1.2 Public Safety Canada

Public Safety Portfolio
• Public Safety Canada (PS) • Canada Border Services Agency (CBSA) • Canadian Security Intelligence Service (CSIS) • Correctional Service Canada (CSC) • Parole Board of Canada (PBC) • Royal Canadian Mounted Police (RCMP) • RCMP External Review Committee (ERC) • Commission for Public Complaints Against the RCMP (CPC) • Office of the Correctional Investigator (OCI)
Organization Priorities
• Improve workplace culture through advancing the implementation of the departmental realignment, transformation activities, and Destination 2020 initiatives. • Lead the federal government's efforts to advance the Canada's Cyber Security Strategy and cybercrime agenda in collaboration with provincial, territorial, private sector and international partners. • Advance the Counter-terrorism Strategy by leading domestic efforts to prevent radicalization. • Modernize the approach to emergency management in Canada to strengthen whole-of-society resilience and improve the government response. • Achieve greater results in community safety by increasing the efficiency and effectiveness of crime prevention, policing and corrections systems. • Continue to strengthen the fundamentals of financial and human resources management to ensure a nimble organization and a sustainable, productive and engaged workforce.

Source: Public Safety Canada (2015b). Report on Plans and Priorities 2015–16, 4–11, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rprt-plns-prrts-2015-16/rprt-plns-prrts-2015-16-en.pdf, Public Safety Canada, 2015–2016. Reproduced with the permission of the Minister of Public Safety and Emergency Preparedness Canada (2015).

Since its inception in 2003, Public Safety Canada's key role has been as a developer of policy and coordinator of programs across one of the largest and most decentralized democracies in the industrial world. PSC works with all levels of Canadian government (federal, provincial, and territorial), community groups, first responders, and the private sector on critical infrastructure issues, national emergency preparedness, and basic community safety. As mentioned above, the National Security Program is within its portfolio. In fulfilling its mission, it allies with other countries and international organizations. A major feature of the work of Public Safety Canada is its collaboration with the United States on infrastructure protection. A potential partnership is with the Department of Homeland Security's Regional Resilience Assessment Program (RRAP). The RRAP became operational in 2015. Its purpose is to identify vulnerabilities and set reliable measures and safety indices for evaluating the risks and addressing the vulnerabilities. It is a nonregulatory and voluntary arrangement that aims to enlist the participation of all levels of government, private-sector stakeholders, and academe.

Table 1.3 Public Safety Canada Organizational Chart


Public Safety Canada Portfolio
Parliament
Minister
Parliamentary Secretary
Deputy Minister and Associate Deputy Minister
Agencies
Review Bodies
Canada Border Services Agency (CBSA)
Royal Canadian Mounted Police (RCMP)
Canadian Security Intelligence Service (CSIS)
Correctional Service Canada (CSIS)
Parole Board of Canada (CSIS)
Public Safety Canada (PS)
Civilian Review and Complaints Commission for the RCMP (CRCC)
Office of the Correctional Investigator (OCI)
RCMP External Review Committee (ERC)

Source: Public Safety Canada. (2015a). About Public Safety Canada, http://www.publicsafety.gc.ca/cnt/bt/index-eng.aspx, Public Safety Canada, 2015. Reproduced with the permission of the Minister of Public Safety and Emergency Preparedness Canada (2015).

BRITAIN In 2008, the British government published its first *National Security Strategy*. In May 2010, a new political administration, on its first day, established a National Security Council (a committee to the Cabinet) and appointed a national security adviser. The Cabinet

Office (2013) defines the National Security Council as "a coordinating body, chaired by the Prime Minister, to integrate the work of the foreign, defence, home, energy and international development departments, and all other arms of government contributing to national security." It is also the main forum for collective discussion of the government's objectives for national security. It attempts to set national-security priorities based on the threat analysis and how best to address them under the prevailing economic conditions and financial climate. The council meets weekly, and the chair is the Prime Minister. The membership includes the following officials:

- Prime Minister
- Deputy Prime Minister
- Chancellor of the Exchequer
- First Secretary of State
- Secretary of State for Foreign and Commonwealth Affairs
- Secretary of State for Defence
- Secretary of State for the Home Department
- Secretary of State for International Development
- Secretary of State for Energy and Climate Change
- Chief Secretary to the Treasury
- Minister for Government Policy

Other Cabinet ministers attend as required, which depends upon the need for their consultation when relevant matters to their subject fields and offices apply. Similarly, the chief of the defence staff and heads of intelligence agencies also attend when required.

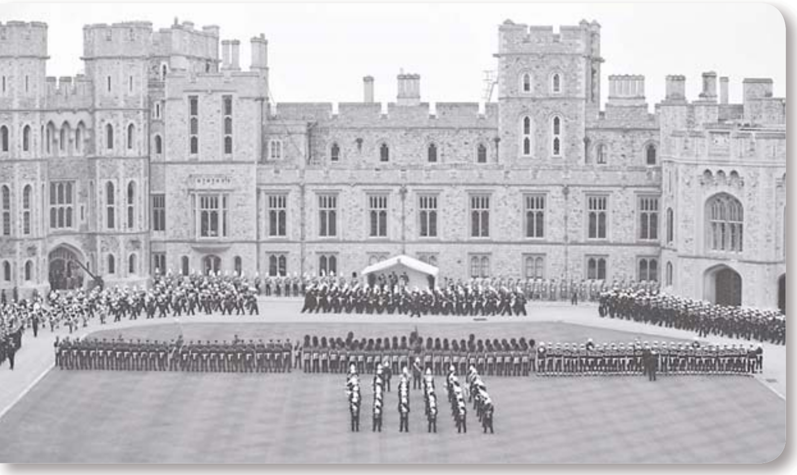
Unfortunately, the Cabinet Office does not define national security. The U.K. Ministry of Defence (2009) defines national security as "the traditional understanding of security as encompassing 'the safety of a state or organization and its protection from both external and internal threats'" (p. 6).

The national-security strategy document, however, does pose a similar worldview as most governments. The shift away from interstate conflict and conventional military operations is the core theme of the report. Unlike the United States, the changing security environment does not require a reorganization of the national government. Rather, national security can be maintained through the existing apparatus and cross-government collaboration. According to the national-security strategy 2010 report, *A Strong Britain in an Age of Uncertainty*,

> The risk picture is likely to become increasingly diverse. No single risk will dominate. The world described above brings many benefits but can also facilitate threats. Therefore, achieving security will be more complex. During the Cold War we faced an existential threat from a state adversary through largely predictable military or nuclear means. We no longer face such predictable threats. The adversaries we face

will change and diversify as enemies seeks means of threat or attack which are cheaper, more easily accessible, and less attributable than conventional warfare. These include gathering hostile intelligence, cyber attack, the disruption of critical services, and the exercise of malign influence over citizens or governments. (U.K. Cabinet Office, 2010, p. 18)

The Cameron government conducted Britain's first **National Security Risk Assessment** (NSRA) to outline national-security priorities. The findings and prioritization list based its results on degree of likelihood and the severity of impact on the economy, institutions, and infrastructure (see Table 1.4).



British Military Units on Parade

Source: U.K. Ministry of Defence, Copyright © Crown. Retrieved from www.defenceimages.mod.uk.

HOMELAND SECURITY

Canada

Public Safety Canada is formally defined by public safety and emergency preparedness (since 2003) and national security (since 2006) rather than homeland security, but its responsibilities include the national agencies for emergency management and border security, which in the United States fall under DHS. Public Safety Canada is responsible for criminal justice and intelligence too, which in the United States are outside of the DHS.

Britain

The British government has considered a department of homeland security but continues to departmentalize home, foreign, intelligence, and military policies separately. The Home Office is closest to a department of homeland security; it is officially described as "the lead government department for immigration and passports, drugs policy, counter-terrorism and policing" (U.K. Cabinet Office, 2013, n.p.).

United States

THE SECURITY PARADIGM BEFORE 9/11 During the Cold War, homeland security belonged to a scattered mix of federal, state, and local agencies. In all, the apparatus included more than two dozen departments and agencies, with assets distributed among all fifty states (Selbie,

Table 1.4 United Kingdom—National Security Priority of Risks

Tier One
• International terrorism affecting the United Kingdom or its interests, including chemical, biological, radiological, or nuclear attack by terrorists and/or a significant increase in the levels of terrorism relating to Northern Ireland • Cyber attacks on United Kingdom cyberspace and large-scale cybercrime • Major accident or natural hazard which requires a national response, such as severe coastal flooding affecting three or more regions of the United Kingdom or an influenza pandemic • An international military crisis between states, drawing in the United Kingdom and its allies as well as other states and nonstate actors
Tier Two
• Attack on the United Kingdom or its overseas territories by another state or proxy using chemical, biological, radiological, or nuclear (CBRN) weapons • Risk of major instability or overseas wars that creates an environment that terrorists can exploit to threaten the United Kingdom. • A significant increase in the level of organized crime affecting the United Kingdom. • Severe disruption of information received, transmitted, or collected by satellites, possibly as a result of a deliberate attack by another state
Tier Three
• Large-scale military attack on the United Kingdom by another state (not involving the use of CBRN weapons), resulting in fatalities and damage to infrastructure within the United Kingdom. • Significant increase in the level of terrorists, organized criminals, illegal immigrants, and illicit goods trying to cross the border into the United Kingdom. • Disruption of oil or gas supplies to the United Kingdom or price instability due to war, accident, major political upheaval, or deliberate manipulation of supply by producers • Major release of radioactive material from a civil nuclear site within the United Kingdom that affects one or more regions • A conventional attack by a state on another NATO or E.U. member to which the United Kingdom would have to respond • Attack on a United Kingdom overseas territory as a result of sovereignty dispute or wider regional conflict • Short- to medium-term disruption to international supplies of resources (e.g., food or minerals essential to the United Kingdom.)

Source: U.K. Cabinet Office (2010).

2001, p. 10). Border protection, public health, disaster management, law enforcement, and counterespionage were mostly themes and terrain separate from the notion, undertaking, and study of national security.

Several events in the 1990s, however, stirred concerns within government over the potential of terrorist attacks. The 1993 bombing of the World Trade Center, the bombing of the Murrah Federal Building in Oklahoma City in 1995, attacks on U.S. embassies in Kenya and Tanzania in 1998, and the 2000 assault on the USS *Cole* in Yemen created a conclusive body of evidence of a growing threat from networks of terrorists groups who could strike from anywhere in the world and within the United States. In 1999, the U.S. Commission on National Security/21st Century (2001), also known as the Hart-Rudman Commission, recommended overhauling the U.S. Government and civilian personnel system, redesigning executive branch institutions and reassessing and organizing congressional oversight. The commission noted that the era of U.S. invulnerability was closing. The proliferation of unconventional weapons and the asymmetric nature of warfare against terrorism had neutralized America's conventional military dominance.

As the Hart-Rudman Commission warned, at large in the world was access to the materials and expertise required to assemble weapons of mass destruction. The dissolution of the USSR elevated the potential threat from the proliferation of chemical, biological, radiological, and nuclear materials. The dismissal and dispersal of trained scientists and engineers from de-funded government programs led to the dissemination of technical personnel circulating the world in search of new homes for their skills. A global black market (currently in an estimated sum of 10 trillion USD [Nuewirth, 2011]) and the availability of information through open sources or via corruptible channels heightened fears of vulnerability. Against the backdrop of these events and circumstances, the security community began to consider the nation's ability to avert and mitigate the consequences of terrorist attacks. Those concerns concretized on September 11, 2001. Describing the time of the attack, the **9/11 Commission report** (formally known as the *Final Report of the National Commission on Terrorist Attacks Upon the United States*) began Chapter 8 with the line "THE SYSTEM WAS BLINKING RED" (9/11 Commission, 2002, p. 254). Finally, the 9/11 attack lifted the concept of homeland security to a new level of comprehension and created a sense of apprehension in government and among the public. With the suddenness of the attack, U.S. national interests were no longer in Europe, Japan, or in remote corners of the world. Commercial and critical infrastructure assets (such as seaports, energy and communication grids, the food supply, the health system, iconic structures, and anywhere an attack would mean a destruction or disruption of life and daily routine) required an effort for national security.

AN ERA OF NEW GEOPOLITICS At a Unity Luncheon in Atlanta, Georgia, in 2002, George Bush said, "It used to be that the oceans would protect us. But that was all changed on September 11th." The president was referring to the Global War on Terrorism and, by implication, announcing that the geopolitical rivalry was morphing into a new reality where the entire planet was a potential battle space. Using its own words, the Department of Defense (2006) concurred with Bush's assessment.

> Throughout much of its history, the United States enjoyed a geographic position of strategic insularity. The oceans and uncontested borders permitted rapid economic growth and allowed the United States to spend little at home to defend against foreign threats. The advent of long-range bombers and missiles, nuclear weapons, and more recently of terrorist groups with global reach, fundamentally changed the relationship between U.S. geography and security. Geographic insularity no longer confers security. (p. 24)

As technology was making the world smaller by crushing time and territory, it was also enabling state and nonstate adversaries with the same tools. The incorporation of the latest technological advancements has always been a challenge for all militaries. In the post–Cold War era, however, never has the pace of technological change been so great or **geopolitics** so complex. The term *revolution in military affairs* (RMA) is a recurring and loose theme to describe the process of integrating technological innovations in weapon systems. In the discourse over RMA, the primary focus is on the important changes created by computer technologies and communication systems (Dalby, 2009). The array of new generation weaponry was on display during the 1991 Gulf War. The use of "smart" weapons, which were supported by global positioning navigation systems and the latest information technology (IT), allowed allied forces to outmaneuver the opposition, destroy targets, and limit casualties (Dalby, 2009). This technology not only wrought changes in military arms but also in military organization and culture.

The **revolution in military affairs** began to gain notice during the 1970s. The increasing accuracy and effect of new munitions at the end of the Vietnam War and in Middle East conflicts was observable. One noted observer was the Soviet Chief of Staff Marshall Nikolai Ogarkov. In the 1980s, Ogarkov wrote about the "military technical revolution" he was witnessing. He viewed the trend as a threat to Warsaw Pact forces whose major advantage was in the number of military assets, not in the technological or computerized sophistication of its weapons. Experts often cite Ogarkov's writings and warnings to his government as the genesis of the current thinking on RMA (Chapman, 2003). However, his views were not singular to him. In 1970, two years before the invention of the microchip, General William Westmoreland, testifying in Congress, reported on the USSR's fear of the U.S.'s mounting advantage. He outlined his expectations for the nature of prospective military conflict, saying, "On the battlefield of the future, enemy forces will be located, tracked and targeted almost instantaneously through the use of data links, computer assisted intelligence evaluation, and automated fire control" (quoted in Chapman, 2003, p. 2).

Thus, RMA refers to the precision weapons and information technology of modern warfare needed to attain decisive military action without the need for large mobilized land forces. It is a system of systems, often referred to as C4ISR (command, control, communication, computers, intelligence, surveillance, and reconnaissance). C4ISR combines information collection, analysis, and transmission and weapons systems to create perfected mission assignment—or what others sarcastically have called "precision violence" or "just-in-time warfare" (Kaldor, 2001). The evolution of warfare technology creates a new fast-paced battlefield. Success on this battlescape ideally requires an integration of hyperaccurate reconnaissance, seamless intelligence, the most advanced standoff munitions (laser- or T.V.-guided missiles), and computers (Bolkom, 2000; Jordan et al., 2009, p. 318).

The key elements to having this advantage are enhanced command systems and situational awareness. Remote sensors and computer tracking of numerous targets allow for smaller, more flexible units to cover more distance by having the ability to interoperate and form into joint operations. This means a shift away from division-centric command structure to take advantage of precision navigation systems and precision air power (Jordan et al., 2009, p. 318). This sort of flexibility comes not only from the ability to adapt to technology but also from the ability to adapt change-management strategies operationally, organizationally, and according to regional and local environments (as in Afghanistan, where special forces units used horse transportation and laser targeting technology to track enemy movements). Theoretically, it also means no territory is remote and anywhere on earth is within reach at nearly any time. Geopolitics in this arena is no longer framed by an interstate system of borders and inviolate state sovereignty. Rather, it implies a field of global conflict involving state and nonstate actors, of disparate regional and strategic contests, and a struggle that targets political and economic objectives without the ideological passions of the past.

When Bush made his pithy comments, he was simultaneously discussing the new military arena, the "transformational military" his Secretary of Defense Donald Rumsfeld was advocating, and the terrestrial and earth-orbit technology that was driving events. The reorganization of the armed services into smaller brigade-sized units makes possible rapid deployment surges into global flash points and trouble spots. Therefore, the traditional organization of the service branches into separate missions and roles yielded to a new priority based upon joint operations (Dalby, 2009). However, despite the technological superiority of U.S. forces, the dependency on C4ISR systems makes the "transformed" military vulnerable. The ability to react faster because of superior intelligence gathering and synchronization methods comes with a risk. The disruption of the hi-tech military infrastructure can affect the delicate efficiencies of space-based communication and monitoring satellites and, in turn, the coordination of ground conditions and operations.

These same strategies also put homeland security on alert. As a way of compensating for the U.S. technological lead, peer competitors may choose to adapt strategies directed at nonmilitary targets. In commercial and private life, Americans have become highly dependent upon technology. The critical infrastructures of financial systems, energy grids, communication networks, commercial transportation, supply chains, and the food supply are strategic targets. These new asymmetric threat assumptions pertain to not only nonstate actors but also to near peer competition with established and rising states. As U.S. dependence on these systems has grown, economic, social, and security stability is targeted and made more vulnerable. The use of cyber terrorism, biochemical attacks, and the acquisition or development of WMDs can be part of strategies that, conjecturally and in reality, pose counter and pre-emptive strike options. An opposition force that is in a position of weakness, conventionally or technologically, will have these alternatives to consider. The overall national-security strategy must reflect these contingencies and provide for the systemic redundancy and resiliency needed to sustain and attack as well as have in place the capability to deter and retaliate.

RMA also makes the process of budgeting and planning for future conflict more complex. The advent of breakthrough or disruptive technology can erupt anytime and tilt the balance of power in one direction or another. Despite the degree of impossibility, national-security policy has to find a way to prepare for such events. Forecasting the future is even more challenging given the pace of technological advancement and the pattern of change, where the ability to defend is trailing the capability to attack.

NEW CONFLICT ARENA At the end of the World War II, the United States found itself at the center of world affairs. In order to counter the Soviet threat, the authors of **NSC-68** reassessed American foreign and defense policy and determined that conditions required a long-term military buildup in "righting the power balance." Today, the United States still holds

C4ISR

Source: Photo on left by Information Technology/Photo by Bob Mical on Flickr; Photo in middle by Brandon Booth; Photo on right by NASA/JPL-Caltech.

center stage. However, the conflict arena is unfamiliar. It not only involves asymmetric and nonasymmetric armed conflict but also cyber war and climate disruptions. It is, in a very true sense, an **all-hazards** defense strategy. Poverty, migration trends, ecological disasters, organized crime, terrorism, regional conflicts, and disruptive technologies all have an impact on U.S. national security. Any attempt to reshape the future through foreign policy or national-security strategy must consider the new geography of violence and upheaval within a mutating security structure of continuous political tension.

Under such conditions, the policymaking process is complex. Nonetheless, the 9/11 Commission report emphatically made clear that the generation that experienced the 2001 catastrophe must match the effort of the earlier generation of Americans who restructured government to meet the challenges of the 1940s and 1950s. That security structure created a generation ago suits a world that no longer exists. The authors of the report also warn that incremental and *ad hoc* adjustments are inadequate. To date, the overhaul of the system has taken time and success is difficult to measure. The size of the bureaucracy, the scope of national security, and the forces of globalization all contribute to the enormity of the challenge. Despite the obstacles, the national-security strategy has to stipulate, as accurately as possible, the nation's preparation against any of the potential onslaughts.

Among the challenges is the fact that the new era of warfare occurs in areas of failed or frail states. In these jurisdictions, there are the virtual opposite conditions of legitimate, functioning states. They can hoist a national flag, issue a national currency, and declare a right to sovereignty, but control over territory and their monopoly on violence erodes as the administrative apparatus collapses and becomes corrupt (Kaldor, 2001). Modern warfare was an interstate battle between nations, which had no such issues, and hence, victory was basically achieved with the military capture of territory. However, the mere capacity to "kill people and break things" no longer is the essence of these new military conflicts. The purpose of the asymmetric war effort is to continue the violence. Rather than the Clausewitzean motive to "compel an opponent to fulfil our will," the objective, often, is to spread panic and create disorder so that the conditions for economic, political, and criminal exploitation remain apposite. Civilian targets surpass military targets as strike objectives while the military needs to respond as more than a combat force. To be effective, it requires diplomacy, law enforcement capabilities, technological skills, and the ability to administer humanitarian aid. Adapting national-security policy to meet the needs of the new conflict arena requires flexibility and foresight.

If the national-security interests of the United States included, as Dean Acheson asserted, "creating an environment in which free societies may exist and flourish," then those responsibilities required "the long war" of defeating terrorist networks, limiting the proliferation and development of WMDs, and influencing the options of fragile and failed states. It also infers that anywhere on the entire planet is a potential battlefield. The defense of the U.S. homeland must also take into account assaults of nature and the consequences of ecological disaster. How does the United States, then, defend itself in an all-hazards environment of potential natural- and human-inflicted catastrophes if the national-security establishment is often caught in the bureaucratic inertia of fighting the last war? This becomes the systemic challenge.

Adjustment to the new order of world affairs has and will continue to be a process of trial, reorientation, missteps, and lapses. Inhibiting progress are not only the present institutions and embedded interests but also a policymaking apparatus and a preference for large-scale maneuver warfare, which are rooted in a fluctuating interstate system. It is a system that has been reshaped by technology and the demands of an ever expanding and intensifying global economy.

These developments have given way to a different structure and level of interaction. For the national-security establishment, it involves a break from the state-centered international system and contending more with national and subnational governments, quasi-states, ethnic groups, rivalries among traditional allies, criminal gangs, diasporas, nongovernmental organizations, and the new phenomena in media. In the post–Cold War arena of conflict, the security framework of past power alliances and strategies based upon a notion of collective security has become outmoded. The principal that an attack on one member of an alliance presumes an attack on all members loses relevance in face of today's threats. The organizing principles of U.S. national-security strategy reflect less a threat from peer military competitors and more of an all-hazards approach to counter transnational forces that emanate from criminal enterprises, terrorists, pirates, and events caused by natural catastrophes. Yet, while these the emerging threats exist, the primary competitors of the Cold War are still major players. Russia and China are participants and innovators in this asymmetric war. They compete politically and economically with the United States and continue to prosecute the remains of a conflict born from the previous era but with variation in mission and a rationale adapted to the realities of the post–Cold War period. Adding to the enigma and burden of the American security establishment is the need for U.S. hegemony to support global commerce and defend the global commons. Hence, the role of the national security–homeland security establishment is more complex than in the past and subject to unprecedented pressures from varied and new sources.

THE ORIGIN OF THE U.S. DEPARTMENT OF HOMELAND SECURITY Justified mostly as a response to the international terrorist attacks of September 11, 2001 (9/11), on September 20, 2001, President George W. Bush announced that by executive order, he would establish an Office of Homeland Security within the White House. The actual order (13228) was issued on October 8. The office was established under the direction of Tom Ridge, formerly governor of Pennsylvania, with few staff and no budget for distribution. The Homeland Security Act of November 25, 2002, established, effective January 2003, a department (DHS) that absorbed 22 prior agencies—the largest reorganization of the U.S. government since the establishment of the Department of Defense in 1949. The Office of Homeland Security dissolved, and the new department, with a total of over 180,000 employees, became the third largest in the U.S. government.

Bush also sought stronger executive powers, partly in the name of homeland security. On October 29, Bush issued the first Homeland Security Presidential Directive (HSPD). He would issue a total of 25 before leaving office in January 2009; during his two terms, he issued 66 National Security Presidential Directives, almost all of them after 9/11. On September 24, 2001, Bush announced the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act. This became the **USA PATRIOT Act**, which Congress approved with little deliberation (normally a bill of such length and consequence would be debated for years). The president signed it into law on October 26. The act was long and conflated many issues but primarily increased the government's surveillance and investigative powers in order to "deter and punish terrorist acts in the United States and around the world." The legislation also included the legal right to monitor credit card transactions, telephone calls, academic transcripts, drug prescriptions, driving licenses, bank accounts, airline tickets, parking permits, websites, and e-mails. The Patriot Act raised severe criticism. The expansion of government authority in redefining terrorist-related crimes and facilitating information sharing between local law enforcement and the intelligence communities were tested in the courts. Although the act provides for congressional oversight, opponents often warn and contest its potential threat for abuse and the danger it poses to individual privacy rights (Sauter & Carafano, 2005). To varying degrees, these arguments have successfully withstood challenges.

In the first executive order on October 8, 2001, in many executive justifications, and in popular understanding, homeland security was equated with counterterrorism, but counterterrorism was always a minor part of departmentalized homeland security. Before 9/11, 46 federal agencies had some counterterrorist responsibilities, according to the Congressional Research Service at the time (Perl, 2002, p. 9). DHS absorbed few of them. Then, as now, U.S. counterterrorism is conducted mostly by the intelligence agencies, the military services, the Federal Bureau of Investigation, and state and local law enforcement agencies, all of which lie outside of DHS, although they coordinate. Most of DHS's subordinate departments and activities manage border security, immigration, tariffs and customs, security within American waters, the security of infrastructure, natural risks, and emergencies in general.

The establishment of DHS popularized the term *homeland security*. From 2001 to 2008, according to Google Ngram, use of the term *homeland security* rose from relative obscurity to surpass use of *national security*. Almost all observers agree, however, that despite the years and waves of events and the massive investment, there is no single definition of homeland security. For some commentators, the term itself is embarrassing and misleading. For Benjamin Friedman, the term helps justify excessive, cost-ineffective investments in countering terrorism.

Similarly, we have no standard and effective homeland security strategy. For over a decade, iterations of these concepts have been illusive, and attempts to give them form appear in a sequence of official documents. However, no standard strategic statement has emerged. Critics complain that the effort to form a simple, clearly stated definition and an organizing homeland security strategy is hampered by a failure to (1) establish a set of national priorities, (2) identify resources for deployment and response to events, (3) align definitions with missions across an array of disparate federal and subfederal entities, and (4) address risk mitigation associated with

Table 1.5 Mission Areas of Homeland Security as Specified by the *National Strategy for Homeland Security* and Required by the Office of Management and Budget (OMB) for All Entities Submitting Budget Requests

2003 *National Strategy for Homeland Security*

- Intelligence and warning
- Border and transportation security
- Domestic counterterrorism
- Protecting critical infrastructure
- Defending against catastrophic events
- Emergency preparedness and response

2007 *National Strategy for Homeland Security*

- Prevent and disrupt terrorist attacks
- Protect the American people, critical infrastructure, and key resources
- Respond and recover from incidents that do occur

Source: Compiled from data from U.S. Homeland Security Council (2007).

the full range of threats. As a result, funding is inefficiently skewed and driven by availability and donor resources. Oversight is inadequate. A verdict by the Congressional Research Service in 2013 concluded,

> Definitions and missions are part of strategy development. Policymakers develop strategy by identifying national interests, prioritizing goals to achieve those national interests, and arraying instruments of national power to achieve the

COMPARATIVE PERSPECTIVES

BOX 1.5

Homeland security means domestic efforts to stop terrorism or mitigate its consequences. In that sense, the name of the Department of Homeland Security misleads. Much of what DHS does is not homeland security, and much of its budget does not count as homeland security spending, according to the Office of Management of Budget [sic]. I use the "odiously Teutono/Soviet" phrase "homeland security" with regret, only because it is so common. Only a nation that defines its security excessively needs to modify the word "security" to describe defense of its territory. In most nations, "security" or "defense" would suffice. (Friedman, 2010, p. 186)

> national interests. Developing an effective homeland security strategy, however, may be complicated if the key concept of homeland security is not defined and its missions are not aligned and synchronized among different federal entities with homeland security responsibilities. (Reese, 2013, n.p.)

The White House and DHS draft the primary documents that frame strategic homeland security policy (Reese, 2013). The Bush administration's 2002 and 2007 *National Strategies for Homeland Security* contained the accepted guiding principles during their tenure. The Obama administration's *2010 National Security Strategy* displaces the previous judgments put forth by the Bush White House, and added to the body of literature in 2011 with the release of the *National Strategy for Counter-Terrorism*.

The Department of Homeland Security produces strategic documents. However, DHS literature mostly focuses on departmental purview, not the more holistic issues of homeland security missions and responsibilities across the spectrum of federal and subfederal entities and jurisdictions.

The documents below form the list of official interpretations regarding the definition and mission statement of the American concept of *homeland security*. They all differ in focus, emphasis, and perceptions of what constitute clear and present threats. Although they converge on many points, each is sensitive to the historical moment and colored by political nuance.

- *2003 National Strategies for Homeland Security*
- *2007 National Strategies for Homeland Security*
- *2008 Department of Homeland Security Strategic Plan*
- *2010 National Security Strategy* (supersedes *2007* document)
- *2010 Bottom-Up Review*
- *2010 Quadrennial Homeland Security Review*
- *2011 National Strategy for Counter-Terrorism*

Rather than regard the domain of U.S. homeland security as a failure in the alignment of missions, resources, and national priorities, there are others who prefer to assess the situation more hopefully. They view homeland security as an evolving ecosystem rather than a complicated apparatus with custom parts tightly fitted to achieve a specific purpose. They reason that the lack of a common vision and vernacular allows the organism to find its own direction and form its shape. Under such design, whether intentional or inadvertent, homeland security forms more naturally from the ground up. This would be a counterconstruction of the national-security establishment, which is top-driven and highly centralized. Agreement is not always a blueprint for success. As Christopher Bellavita observes,

> Other important and often used terms—like terrorism, justice, disaster, or emergency management—also do not have single definitions. Yet we make progress

Table 1.6 Summary of Homeland Security Definitions

Document	Definition
2007 National Strategy for Homeland Security (White House)	A concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that occur
2008 U.S. Department of Homeland Security Strategic Plan 2008–2013 (DHS)	A unified effort to prevent and deter terrorist attacks, protect and respond to hazards, and to secure the national borders
2010 National Security Strategy (White House)	A seamless coordination between federal, state, and local governments to prevent, protect against, and respond to threats and natural disasters
2010 Quadrennial Homeland Security Review (DHS)	A concerted national effort to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards where American interests, aspirations, and way of life can thrive
2010 Bottom-Up Review (DHS)	Preventing terrorism, responding to and recovering from natural disasters, customs enforcement and collections of customs revenue, administration of legal immigration services, safety and stewardship of the nation's waterways and marine transportation system, as well as other legacy missions of the various components of DHS
2011 National Strategy for Counter-Terrorism (White House)	Defensive efforts to counter terrorist threats
2012 Strategic Plan (DHS)	Efforts to ensure the homeland is safe, secure, and resilient against terrorism and other hazards

Source: Reese (2013, p. 8).

Table 1.7 Summary of Homeland Security Mission and Goals

Document	Mission and Goals
2007 National Strategy for Homeland Security (White House)	• Prevent and disrupt terrorist attacks • Protect the American people, critical infrastructure, and key resources • Respond to and recover from incidents • Strengthen foundations for the long term

Document	Mission and Goals
2008 U.S. Department of Homeland Security Strategic Plan 2008–2013 (DHS)	• Protect the nation from dangerous people • Protect the nation from dangerous goods • Protect critical infrastructure • Strengthen preparedness and emergency response capabilities • Strengthen and unify DHS operations and management
2010 National Security Strategy (White House)	• Strengthen national capacity • Ensure security and prosperity at home • Secure cyberspace • Ensure American economic prosperity
2010 Quadrennial Homeland Security Review (DHS)	• Prevent terrorism and enhance security • Secure and manage the borders • Enforce and administer immigration laws • Safeguard and secure cyberspace • Ensure resilience from disasters • Provide essential support to national and economic security
2010 Bottom-Up Review (DHS)	• Prevent terrorism and enhance security • Secure and manage borders • Enforce and manage immigration laws • Safeguard and secure cyberspace • Ensure resilience from disasters • Improve departmental management and accountability
2011 National Strategy for Homeland Security (White House)	• Protect the American people, homeland, and American interests • Eliminate threats to the American people's, homeland's, and interests' physical safety • Counter threats to global peace and security • Promote and protect U.S. interests around the globe
2012 U.S. Department of Homeland Security Strategic Plan 2012–2016 (DHS)	• Preventing terrorism and enhancing security • Securing and managing borders • Enforcing and administering immigration laws • Safeguarding and securing cyberspace • Ensuring resilience from disasters • Providing essential support to national and economic security

Source: Reese (2013, p. 11).

> in understanding and using each of those ideas. The absence of agreement can be seen as grist for the continued evolution of homeland security as a practice and an idea. (Bellavita, p. 20)

One of the purposes of the study of homeland security is to offer some estimation of the objective reality and the institutions in place to execute policies and perform the missions related to *security*. In the process, the student will examine alternative definitions and issues and describe the entities charged with policy formulation and implementation while reviewing the origins and evolution of homeland security. It will be for the reader to decide how best to frame analysis. Is homeland security an organ of the state whose structure seeks to adapt to the changing environment of natural hazards and human conflict? Or is it best to assume it is an evolving social construction responding to stimuli?

THE U.S. HOMELAND SECURITY ESTABLISHMENT When the Homeland Security Act established the Department of Homeland Security, it not only set loose the greatest reorganization of government since 1949, it also stirred fears of governmental over-reach, abuse of power, and questions of whether a federal administrative body was up to the task of such a managerial test. The creation of the Department of Homeland Security was an effort to centralize responsibility and accountability under a single organizational body. It was also reasoned that information and intelligence sharing, enhanced national preparedness, and resiliency would improve under a central structure. Planners assumed the current arrangement of a scattered and uncoordinated network of command and control was a systemic weakness. Some success has been achieved. However, critics also note persistent weaknesses in program development, interoperability, execution, and even organizational culture.

The executive order of October 8, 2001, creating the **Homeland Security Council** (HSC) included a purpose statement that read as follows: "to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."* The president's Homeland Security Council included a membership of no more than 21 people, selected from the private sector, academia, officials, and nongovernmental organizations. Four Senior Advisory Committees for Homeland Security—State and Local Officials; Academia and Policy Research; Private Sector; and Emergency Services, Law Enforcement, and Public Health and Hospitals—form the core of the advisory body.

As defined, the Homeland Security Council is an advisory body that meets at the discretion of the President. Its function is to advise the President on all matters relevant to homeland security.

* The HSC was almost the same as the NSC; therefore, the change attracted criticism. "The creation of the HSC essentially **bifurcated** the homeland security process: there were now two agencies reporting to the President that had policy authority over national security issues" (Gaines & Kappeler, 2012, p. 209). In May 2009, President Barack Obama merged the staff of the NSC and HSC, although their separate statutes remain.

Membership includes the assistant to the president for homeland security and counterterrorism, vice president, director of the CIA, secretary of defense, secretary of the treasury, secretary of health and human services, attorney general, director of the FBI, secretary of transportation, and the administrator of the Federal Emergency Management Agency (FEMA). It is an entity within the Executive Office of the President. As with the NSC, membership includes statutory and nonstatutory members.

One of the outcomes of the attacks of 9/11 and in the recommendations by the 9/11 Commission report was the establishment of the Office of the **Director of National Intelligence**. The Intelligence Reform and Terrorist Prevention Act of 2004 created the position of the director of national intelligence (DNI). The legislation replaced the director of the CIA as the principal advisor on intelligence matters. The bill, in effect, created another layer of bureaucracy atop the intelligence community structure (Jordan et al., 2009, p. 128). How this will provide a centralized coordination process and a more efficient pattern of operation for intelligence gathering remains yet unanswered (Sarkesian, Williams, & Cimbala, 2008, p. 145). Critics claim that because of the reorganization, the NSA and the Defense Intelligence Agency (DIA), although having reporting responsibility to the DNI, are outside the agency's control. Combined, these two organizations, plus the NSA and DIA, account for 80% of the government's intelligence budget (Jordan et al., 2009). Altogether, they account for a major part and effort of the intelligence community. Part of the DNI's role includes control over the national intelligence budget, but the main collection agencies remain within DOD. As Senator John Rockefeller put it,

> We gave the DNI the authority to build the national intelligence budget, but we left the execution of the budget with the agencies. We gave the DNI tremendous responsibility. The question is, did we give the DNI enough authority to exercise his responsibility? (Senate Select Committee on Intelligence, 2007)

Although the CIA continues to be the major intelligence agency, the Director of National Intelligence is the chief coordinator, manager, and chief advisor to the president on intelligence matters. Additionally, not only must the DNI maintain a harmonized working relationship across the broad gamut of all U.S. intelligence-gathering agencies, the office must also build and maintain working relationships with foreign intelligence services. These ties are not restricted to allies but might occasionally include adversary states, too. The structure and operational success depends heavily upon the managerial and diplomatic skills of the director (Sarkesian et al., 2008, p. 148). Until an atmosphere of trust and familiarity settles in, the office and working arrangement will be subject to tensions.

Prior to the global war on terrorism, intelligence gathering had mostly been a matter for foreign policy rather than domestic policy (Samuels, 2006, p. 358). The events on 9/11, however, forced policymakers to reassess the current structure of agency collaboration, command, and control. The Bush administration recognized a need for effective information sharing and integration of intelligence from not only foreign and electronic surveillance operations but also links with local law enforcement. Because of constitutional restrictions about spying on U.S. citizens, the new powers raise serious legal questions.

New York City—September 11, 2001

Source: 9/11 WTC Photo by 9/11 Photos on Flickr.

The FBI is the primary government agency tasked with counterintelligence; however, several other government offices also have responsibilities in the same area. The Office of Intelligence Analysis is an entity within DHS that oversees and coordinates operations throughout DHS, elements of the intelligence community, and between state and local authorities involved with counterintelligence. Additionally, states and major urban areas maintain their own intelligence operations. Known as fusion centers, subfederal level intelligence gathering stations focus on situational awareness and threat analysis to monitor and uncover terrorist threats. Not only do fusion centers concentrate on working to pursue, disrupt, and identify precursor crime and activity relative to emerging terrorist threats, they also work with private-sector personnel and public-safety officials on critical infrastructure protection, disaster recovery, and emergency response events.

These methods of police-led intelligence operations are unique to the traditions of counterintelligence. Proponents of the bottom-up approach to intelligence gathering hope that it can be a check against the reverse procedure of the top-down regimen, which can lead to a system of self-serving conveniences "enmeshed in meaningless operations, committed more to bureaucratic efficiency than to the purpose of intelligence" (Sarkesian et al., 2008, p. 155). The Cold War arms race and the invasion of Iraq are examples that some observers point to as clear cases where the blend of policy formulation and policy advocacy at the top have skewed the policymaking and policy-implementation process.

By employing the perspective of local authorities, many hoped that such an approach might ease that risk at the center and lower the potential for adverse outcomes based upon distorted analysis. According to a U.S. Senate subcommittee, however, these subfederal intelligence fusion centers have not fulfilled their promise. A 2012 report accused the majority of the nationwide network of 77 centers of producing "irrelevant, useless, inappropriate intelligence reporting to the DHS" (O'Harrow, 2012). The debate continues between the detractors and defenders of police-led intelligence.

Another way the central government works with local authorities is through the Defense Department's military commands. The homeland security remobilization involved the creation of the U.S. Northern Command. USNORTHCOM is one of the nine combatant commands under the Department of Defense and operates to centralize homeland defense activities. It provides military assistance to civil authorities in the continental United States, Alaska, Puerto Rico, the U.S. Virgin Islands, Mexico, and Canada. The Posse Comitatus

Table 1.8 The U.S. Homeland Security Establishment

President				
Department of Homeland Security	Director of National Intelligence			Homeland Security Council
Management	Deputies			Homeland Security Advisor
Science and Technology	• Collection • Analysis • Acquisition			Vice President
Policy	• Policy plans and requirements			Secretary of Treasury
National Protection and Programs	CIA	Army	NGO	Secretary of Defense
General Council	DIA	Navy	DEA	Attorney General
Legislative Affairs	NSA	USMC	FBI	Secretary of Health and Human Services
Public Affairs	NRO	USAF	DOE	Secretary of Transportation
Inspector General	INR	USCG	Treasury/TFI	Administrator of FEMA
Health Affairs	DHS/Intel			Director, FBI
Operations Coordination				Director, CIA
Citizenship and Immigration Service				
Chief Privacy Officer				
Civil Rights and Civil Liberties				
Counter Narcotics Enforcement				
Federal Law Enforcement Training				
Domestic Nuclear Detection				
Transportation Security Administration				
U.S. Customs and Border Protection				
Immigration and Customs Enforcement				
U.S. Secret Service				
U.S. Coast Guard				
Federal Emergency Management Agency				
Intelligence and Analysis				

Source: Jarmon (2014).

Act, which restricts the role of the U.S. military in domestic affairs, regulates its operations. However, Congress can allow for exceptions to posse comitatus in the event of a national disaster or emergency.

Unlike its allies, who believed their government machinery and personnel adequate to meet the challenges of the global war on terrorism, the United States invested in a complete reorganization of its security establishment. The restructuring, critics claimed, did not address the salient problems of coordination and information sharing. Rather, the new department became a target for those citing its inefficiencies, tolerance of political patronage, and lack of effective policy guidance and success measurements.

THE BUDGETING PROCESS The Office of Management and Budget is critical to the budgeting process. It provides policy guidance, development, and execution assistance to the president government-wide. It also helps to establish order in the budgeting process amid the political turmoil, jurisdictional conflicts, and budget fights within government. By law, the president must present a budget to Congress by the first Monday in February each year. In the spring prior to that date, the OMB conducts a study of the economy and presents the president with its projections. Individual agencies revise current program budgets based upon the guidelines recommended by the OMB. After reviewing these projections, the OMB makes an analysis of programs and budgets. National-security policy formulation occurs as budget levels and projections are being prepared. This process lasts through the spring of the same year, and by the following summer, the president establishes guidelines and targets as a result of the findings. Agencies review the recommendations, make their projections, and resubmit them to the OMB. The president then makes the decision regarding agency budgets and overall budget policy. The final budget document is released after agencies conform to the president's decision and the OMB makes a final review.

Also required by law is the preparation of the **Quadrennial Defense Review** (QDR). The Department of Defense conducts studies and releases the QDR findings every four years. The Clinton administration authorized the first report in 1997. At the time, the document confirmed the U.S. orientation toward conventional war. Traditional doctrine and funding percentages among the branch services remained in place. The 2006 version, on the other hand, called for the preparation of a "long war" against terrorism. Defeating terrorism, preventing the development and acquisition of WMDs, homeland defense, and helping to democratize politically fragile states were the basic principles. Some of the issues future QDR reports will be addressing are potential economic and budget uncertainty, the balance between leverage and entanglement in foreign affairs, the future of the nation's nuclear arsenal, and the national priorities over investment decisions in infrastructure, security, and more. The government released the first Quadrennial Homeland Security Review in 2010. The QHSR serves as a similar tool for policy guidance as the QDR. Both documents set risk-informed priorities for operational planning.

In the budget process, agencies and departments simultaneously cooperate and compete to define needs and recommend funding limits. The absence of a centralized method for establishing policy and the approaches toward achieving goals forces the system to react in such a way. By meting out tasks and expectations, setting deadlines, and putting limits on the range of items for

Table 1.9 FY2012 Appropriations and FY2013 Requests for Homeland Security Mission Funding by Agency (in USD Millions)

Department	2012 Enacted	2013 Request	Total % (2013)
Agriculture	570.1	551.4	0.80
Commerce	289.6	304.1	0.44
Defense	17,358.4	17,955.1	26.05
Education	30.9	35.5	0.05
Energy	1923.3	1874.7	2.72
Health and Human Services	4146.8	4112.2	5.97
Homeland Security	35,214.7	35,533.7	51.57
Housing and Urban Development	3.0	3.0	—
Interior	57.6	56.7	0.08
Justice	4055.4	3992.8	5.79
Labor	46.3	36.6	0.05
State	2283.4	2353.8	3.42
Transportation	246.6	243.3	0.35
Treasury	123.0	121.1	0.18
Veterans Affairs	394.5	383.7	0.56
Corps of Engineers	35.5	35.5	0.05
Environmental Protection Agency	101.8	102.6	0.15
Executive Office of the President	10.4	11.0	0.02
General Services Administration	38.0	59.0	0.09
National Aeronautics and Space Administration	228.9	216.1	0.31
National Science Foundation	443.9	425.9	0.62
Office of Personnel Management	1.3	0.6	—

(Continued)

Table 1.9 (Continued)

Department	2012 Enacted	2013 Request	Total % (2013)
Social Security Administration	234.3	252.1	0.31
District of Columbia	15.0	25.0	0.04
Federal Communication Commission	—	1.7	—
Intelligence Community Management Account	8.8	—	—
National Archives and Records Administration	22.6	22.5	0.03
Nuclear Regulatory Administration	78.4	76.6	0.11
Security and Exchange Commission	8.0	8.0	0.01
Smithsonian Institution	97.0	100.1	0.15
U.S. Holocaust Memorial Museum	11.0	11.0	0.02
TOTAL	67,988.0	68,905.2	100

Source: Painter (2012).

deliberation, the overall process of federal budget procedures allows the system to work despite a highly charged political environment (Jordan et al., 2009, p. 193). As of 2012, the breakdown of homeland security funding was thus:

- Between federal and nonfederal
    - 30 federal entities receiving funds—48%
    - Department of Homeland Security—52
- Within the federal government
    - State and local entities—52%
    - Department of Defense—26%
    - Other federal agencies—22%

THE FUTURE OF DHS In a 2013 *New York Times* editorial, Thomas Kean and Lee Hamilton, Chair and Vice Chair of the 9/11 Commission report, wrote:

> Homeland Security personnel took part in 289 formal House and Senate hearings, involving 28 committees, caucuses and commissions. In 2009 alone, Homeland Security personnel spent the equivalent of 66 work-years responding to questions from Congress, at an estimated cost to taxpayers of $10 million. (n.p.)

▸ New York City—Ground Zero, 2014

Source: U.S. Customs and Border Protection.

DHS has absorbed more federal personnel and departments than any since the creation of the Department of Defense in 1947, but their total budget was reduced. The enabling legislation also prohibited unionization. The DHS was created quickly, without requisite bureaucratic input, and the executive's centralized control was enhanced by the quick appointment of partisan supporters to leadership positions. In 2006, the Office of Personnel Management found that job satisfaction was lowest in the DHS, of all federal departments and agencies (Gaines & Kappeler, 2012, p. 35). Richard Clarke (2008), the president's former special adviser on cybersecurity, complained that

> the chief criteria in designing and managing the major new government enterprise were appearance and politics, not problem solving. The largest federal department created in more than fifty years was slammed together with insufficient resources and regulatory powers. Worse yet, far from recruiting the best managers that government and industry could assemble, it was laced with political hacks and contractors to a degree never seen in any federal agency. (p. 204)

Other authors noted that many of the new subordinate missions (such as FEMA, Coast Guard, and Customs) were dissimilar to counterterrorism and contributed to "mission distortion within the DHS" (Gaines & Kappeler, 2012, p. 34).

> To a great extent, DHS is a work in progress. As homeland security matures as a federal imperative, the DHS will certainly continue to change. It is a natural part of organizational evolution, and if change does not occur, most likely the DHS will in some regards become less effective in pursuing its various missions. (Gaines & Kappeler, 2012, p. 37)

In such a polyvalent threat environment, cultural, diplomatic, economic, and technological issues also vex the policymaking process. As the authors of *American National Security*, the core text in the security studies field, state, “even given national security professionals committed to collaboration, it has become harder to get agencies to act in concert” (Jordan et al., 2009, p. 212).

Despite the effort to establish a system of responsibilities, accountability, guidelines, and time frames, nothing goes “according to the book.” There is no “book.” These influences plus the need to strike a balance politically and economically come together in a mill of government machinery where opinions constantly form and mature around homeland security strategy, personal biases, and real-world events.

COMPARATIVE PERSPECTIVES

BOX 1.6

Comment 1

Richard Clarke, *Your Government Failed You: Breaking the Cycle of National Security Disasters* (2008):

> The creation and the subsequent dysfunction of the Department of Homeland Security is revealing of the reason why the U.S. government fails at national security. For several years, over two administrations of different political parties, people who were engaged in federal management and national security tried to resist a politically motivated drive to seen to “do something” about security through bureaucratic reorganization. When, after 9/11, that drive became irresistible, the chief criteria in designing and managing the major new government enterprise were appearance and politics, not problem solving. The largest federal department in more than fifty years was slammed together with insufficient resources and regulatory powers. Worst yet, far from recruiting the best managers that government and industry could assemble, it was laced with political hacks and contractors to a degree never seen in any federal agency. (p. 204)

Also according to Richard Clarke, White House Chief of Staff Andrew Card and White House Personnel Chief Clay Johnson, who engineered the design of the reorganization, had several clear objectives.

> They wanted to cut federal expenditures. Thus, the budget for the new DHS was less than the combined budgets for the agencies that were transferred to it, which substantially weakened the department’s ability to fulfill its mandates. Second, they emphasized political appointments in the department as opposed to recruiting career experts. Third, they sought to reduce the role of organized federal labor groups, so the enabling legislation prohibited unionization. Finally, they wanted to ensure that the new bureaucracy was created as quickly as possible, which eliminated requisite planning and criticism from bureaucrats who could identify problems or deficiencies with the new organizational plan. In essence, politics and ideology had a significant impact on the department during its early stages of development, which resulted in a number of problems in later years. (quoted in Gaines & Kappeler, 2012, p. 35)

Comment 2

Jeremy Shapiro, “Managing Homeland Security: Develop a Threat-Based Strategy” (2007):

> Policy discussions of homeland security are driven not by rigorous analysis but by fear, perceptions of past mistakes, pork-barrel politics, and an insistence of an invulnerability impossible that can not possible be achieved. It is time for a more analytic, threat-based approach, grounded in concepts of sufficiency, prioritization, and measured effectiveness. . . . [F]ive years into the apparently endless war on terrorism homeland security should evolve from a set of emergency measures into a permanent field of important government policy that, like any other, must justify its allocation of taxpayer funds though solid analysis. (pp. 1–2)

FINAL CASE STUDY

Should the DHS Be Abolished?

Michael D. Tanner and Christian Beckner

Yes, says Michael D. Tanner, a Senior Fellow at the Cato Institute.

> The creation of the DHS was a classic example of how Washington reacts to a crisis. In the wake of 9/11, the pressure was on Congress and the Bush administration to “do something,” or at least look as if they were doing something. The result was a new Cabinet-level agency that cobbled together a host of disparate agencies, ranging from the Federal Emergency Management Administration (FEMA) to the Fish and Wildlife Service. Nearly every federal employee who wore a badge was simply swept up and dumped into the new bureaucracy. From a simple management or “span of control” perspective, lumping together so many unrelated functions is an invitation to failure.
>
> From a national-security standpoint, the DHS is part of the problem, not the solution. After all, the agencies primarily responsible for counter-terrorism, such as the FBI, CIA, and NSA, are not part of the DHS. This, of course, hasn’t stopped the DHS from developing its own counter-terrorism infrastructure. But, if one of the primary intelligence gaps before 9/11 was the failure of agencies to share information and coordinate activities, it is hard to see how more duplication and fragmentation makes things better.
>
> Making matters worse, virtually every congressman wants to be part of protecting the homeland too. No fewer than 90 congressional committees and subcommittees oversee some aspect of the department.

(Continued)

(Continued)

> With so much of Congress involved—and because no one wants to appear soft on protecting the homeland—spending has skyrocketed, tripling from $18 billion per year in 2002 to more than $54 billion last year [2014]. Money spreads to every congressional district without regard to actual security needs. Thus, the DHS has provided grants to such obvious terrorist targets as Bridgeport, Conn., Toledo, Ohio, and North Pole, Alaska.
>
> Its workforce expanded from 163,000 employees in 2004 to 190,000 by 2014. And far from being efficient, the DHS is regarded as one of the most poorly managed agencies in Washington.
>
> Government audits routinely find the DHS guilty of waste and mismanagement. The Government Accountability Office has for years included the DHS on its list of "high risk" government agencies. A 2010 National Academy of Sciences report accused the agency of failing to rigorously evaluate projects to see whether the benefits outweigh the costs. Many of the 22 agencies falling under the DHS umbrella are among the most dysfunctional in government, including FEMA, the TSA, and the Secret Service. (Tanner, 2015, n.p.)

No, says Christian Beckner, Deputy Director, Center for Cyber and Homeland Security at George Washington University.

> First, and most importantly, the Department in many respects has become much more than the sum of its parts in the last decade, with respect to its operational mission performance. CBP, ICE, USCIS and the Coast Guard all work together to carry out the Department's border security and immigration missions. CBP, TSA and ICE all work together to prevent terrorist and other illicit travel (e.g. human trafficking) to the United States. FEMA and the Coast Guard have become closer since DHS was created in terms of their disaster response roles, and other operational components have been called on to support major disaster response efforts. ICE, the Secret Service, and NPPD all have significant cybersecurity responsibilities, and are working more closely together in support of their respective cyber activities. And all of the operational entities of DHS have some role (although admittedly not the lead federal role) in counterterrorism, and DHS information has played a critical role in disrupting several of the higher-profile terrorist plots targeting the United States over the past 7–8 years.
>
> Second, the Department has played the critical federal role since its inception in integrating state and local law enforcement and first responders into supporting its missions. This is true not only with respect to FEMA and disaster response, but equally importantly with respect to counterterrorism, and increasingly in the last few years with respect to cybersecurity. (Of note on this issue, contrary to the CATO piece, fusion centers are not "operated by

the DHS"—they are entities owned and operated by state and local governments, each with a small number of federal employees detailed by DHS and DOJ.)

Third, stories such as this promote a distorted perspective on the growth of DHS over the past thirteen years. The story says that "spending has skyrocketed, tripling from $18 billion per year in 2002 to more than $54 billion last year." This statistic likely refers to the OMB's government-wide crosscut of homeland security spending, but that annual analysis is not solely about DHS; OMB's numbers include items such as domestic force protection at the Department of Defense and biosecurity programs at HHS. In reality, the DHS budget has grown since its inception from $36 billion in FY 2002 to $55 billion in FY 2011—but this growth rate is far from a "tripling" of the budget. (Budget numbers taken from DHS's response to a Question for the Record by Sen. Ron Johnson from a 2011 Senate hearing. See numbered pages 1029–1031 of this very large PDF.)

It's also worth noting that most of this growth was not due to sprawling bureaucracy but due to increases to frontline operational capacity, in terms of personnel (notably the doubling of the size of the Border Patrol), technology and infrastructure. The reality is that the parts of DHS that I would consider to be "headquarters"—the Office of the Secretary and Executive Management (OSEM), the Office of the Undersecretary of Management, the Offices of Operations Coordination and Intelligence Analysis, and the Science and Technology Directorate—account for only 1.7% of the DHS workforce, a large share of whom are carrying out government-wide Congressional mandates in areas such as IT management and financial oversight.

Fourth, anyone who proposes dismantling DHS should have the burden of proposing what they would do with its constituent parts, and how such an initiative would improve the performance of the Department's current missions. The five entities that have responsibility for immigration, border security and travel security (CBP, ICE, USCIS, Coast Guard, TSA), where the rationale for operational integration is strongest, account for 195,000 of the Department's 225,000 employees—around 87%. Is the author proposing that these five entities should not be within the same Cabinet department? If he is, he's making a proposal that will have a serious negative impact on the government's performance of these missions. If he is not, then he's not really proposing to break up DHS, but instead proposing a more moderate tinkering, perhaps by returning the Secret Service to the Treasury or making FEMA an independent agency again. I wouldn't recommend either of these; in particular, I think FEMA is now critically interlinked with many other parts of DHS. The reality is that there is no realistic option for a major overhaul of DHS that does not have significant operational impacts. (Beckner, 2015, n.p.)

Under these conditions, the term *homeland security* has many definitional variants filled with political nuance and professional and personal bias. Tensions exist due to the dilemmas regarding the choices between security versus freely flowing commerce, evolving policy versus embedded interests, domestic and foreign affairs, and—unavoidably—funding.

Finally, risk positions are complex. They are subject to culture and local capabilities. Attaining a balance between vulnerabilities and resources is at the core of homeland security strategy. In the international domain, countries craft policy and enact laws according to their estimation of specific threats, assessment of available resources, and notions about acceptable loss. There is no standard metric for calculating these factors or forming evaluations. Therefore, a final balance may also be struck between the imperative to have sharply defined and communicated definitions and mission statements that are top-driven and the need to develop a maturing security ecosystem from the ground up.

CHAPTER SUMMARY

This chapter has

- Discussed the various definitions of *security* and the various jurisdictional domains where they apply
- Touched upon the sundry disciplines, fields, and subfields that cover security as a topic
- Defined *human security* and the importance of the *stable state*
- Examined the difference and overlap of interpretations of the meaning between the terms *national security* and *international security*
- Discussed the differences in the missions and organizational structures of the national-security establishment in the United States, Canada, and Britain
- Discussed how the concept of homeland security influenced notions of national security in the United States, Canada, and Britain
- Discussed the impact of the revolution in military affairs on geopolitics, national security, and homeland security
- Reviewed the origins and rationale for the creation of the U.S. Department of Homeland Security
- Described the budgeting process of the U.S. Department of Homeland Security

KEY TERMS

All hazards *21*
Bifurcate *28*
Collective security *2*
Director of National Intelligence *29*
Emergency management *12*
Geopolitics *19*
Homeland Security Council *28*
Human security *7*

Machtpolitik 2

National Security Risk Assessment 16

NSC-68 20

Public Safety Canada 5

Quadrennial Defense Review 32

Revolution in military affairs 19

The 9/11 Commission report 18

USA PATRIOT Act 23

QUESTIONS AND EXERCISES

1. What is the definition of collective security and how has its meaning or nuance changed under the definitions of homeland security?
2. Describe the notion of security as it relates to the various primary domains.
3. What are the influencers that impact the setting of homeland security strategy as opposed to national-security policy?
4. How does Public Safety Canada align with the U.S. Department of Homeland Security? And how does it reflect Canada's federal system and unique geographical placement?
5. What is the difference between homeland security and national security in Britain?
6. In what ways does the security establishment in Britain correspond to that of the United States? And how does it set itself apart from its major ally?
7. What are the differences, similarities, and overlap between the National Security Council and the Homeland Security Council?
8. What do you believe the reasons are for no single, standard Department of Homeland Security strategy or definition of homeland security?
9. How has the revolution in military affairs influenced the security structure of the legacy national-security establishment and the development of homeland security?
10. How do we assess risk and what are the elements that shape strategy?
11. What is meant by a *homeland security ecosystem*?