

# XV

---

---

## Fourth Dimensional Intelligence

### Thoughts on Espionage, Law, and Cyberspace

---

---

David M. Crane\*

*The enemy will be different. . . . No longer will it be the simple terrorist armed with an AK-47 or the Semtex bomb . . . the new threat will be groups who will bond in cyber space and attack using the new weapons of war: viruses, bugs, worms and logic bombs.<sup>1</sup>*

The front cover of a recent *Armed Forces Journal* has an American soldier on a rope bridge suspended over a chasm with the title "Ready for What?"<sup>2</sup> This is a key question for national security policy makers regarding the mission of US Armed Forces as the world moves into the uncharted waters of the new millennium.<sup>3</sup>

Institutionally, the national security structure of the United States is facing many challenges. Configured to meet the Soviet threat, the Armed Forces, as well as the intelligence community, are realizing that changes must be made.<sup>4</sup> The question posed above, however, is relevant regarding the issue of being ready for the next threat. What are the threats that face our national security and how should we be organized functionally to meet those challenges, particularly as they relate to the dimension of cyberspace?

The geopolitical world of the 20<sup>th</sup> Century, drawn along colonial and ideological lines, is fading into the past. The threats faced by the United States today

The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy, or Dept. of Defense.

are not just standing industrial age armies, but international criminals, terrorists, and State and non-State actors using relatively inexpensive and easily attained technology to manufacture weapons of mass destruction.<sup>5</sup>

Throughout history, man has waged warfare, conducted commerce, and established an international political regime in a three-dimensional environment. Mankind has faced and conquered the land, the sea, and the air above, moving freely about in these dimensions. Yet mankind has created another dimension which will shape its evolution well past the start of this millennium. That dimension is cyberspace. It is in this dimension that both the legal and intelligence communities, among others, will have to develop an ability to operate.

Among the practices of States, intelligence gathering is accepted as a necessity in conducting foreign relations.<sup>6</sup> Throughout history, State actors have been collecting information on the intentions, capabilities, and policies of both friendly and rival States.<sup>7</sup>

In the information age, intelligence plays an increasingly important role.<sup>8</sup> Information is the new strategic high ground. For the past fifty years or so the intelligence community of the United States focused on the Soviet Union and its allies, mainly the Warsaw Pact countries.<sup>9</sup> The mission was clear and the community organized itself accordingly to provide critical information to the National Command Authorities<sup>10</sup> on Soviet capabilities and intentions.<sup>11</sup> This organizational model, however, may no longer be valid.<sup>12</sup>

Due to the ever-increasing challenges in gathering that information against a hard target, the community began to rely more and more on its technical capabilities. Imagery intelligence and signals intelligence provided spectacular coverage and monitoring of Soviet communications and critical strategic targets.<sup>13</sup> At times this was at the expense of the other intelligence collection methods such as human-source intelligence (HUMINT).<sup>14</sup> In the asymmetric world of the 21st Century, HUMINT and open source intelligence (OSINT) will play a key role.<sup>15</sup> This role will not change in the dimension of cyberspace and computer network attack or defense.<sup>16</sup> Additionally, the computer will become a useful tool for an intelligence operative or analyst to use.<sup>17</sup>

Throughout our history, however, the role of intelligence in defending our nation has been misunderstood.<sup>18</sup> The methodologies of intelligence gathering can, to some citizens, appear to run counter to the basic principles of a free and open society.<sup>19</sup> Though Americans are fascinated by the capabilities of the community, they have an unrealistic romantic view of the often dangerous and dirty world of intelligence gathering.<sup>20</sup>

## **The Role of Intelligence in the United States**

Until the Second World War, US intelligence played a minor role in protecting our national security. Only during time of war did an intelligence service emerge to support the commander in the field. After the emergency, the intelligence capabilities of the US diminished or were disbanded.<sup>21</sup>

Counterintelligence played even less of a role and was largely nonexistent prior to the First World War.<sup>22</sup> Domestically, the counterintelligence service became a profession in the 1920s with the advent of the Bureau of Investigation in the Department of Justice (later the Federal Bureau of Investigation) and the creation of various service counterintelligence organizations.<sup>23</sup>

The intelligence community has also had an awkward relationship with the Congress. Until the mid-1970s, Congress deferred to the executive branch on issues of national security as a constitutional prerogative of the President acting as Commander-in-Chief.<sup>24</sup> In the early 1970s, allegations of wrongdoing by the intelligence community caused a public outcry and resulted in long-term congressional and presidential scrutiny.<sup>25</sup> The result was the creation of the congressional intelligence oversight committees and presidential guidelines on the proper conduct of intelligence operations, particularly as they related to US persons.<sup>26</sup> Those policies and regulations are still in place and govern the intelligence activities discussed later in this chapter.

Thus, the US intelligence community truly was a creature of the Cold War designed to operate in three dimensions.<sup>27</sup> It was created and designed to counter Soviet hegemony, largely an industrial age threat. With the dissolution of the Soviet Union, and the advent of the information age, the intelligence community, a large and cumbersome bureaucracy, has to evolve into a quick reacting, forward thinking, and agile grouping of agencies ready to respond to various asymmetric threats, including computer network attack.<sup>28</sup>

## **The Challenges Ahead for US Intelligence and Cyberspace**

The need for information by policy makers and warfighters will only increase. The National Command Authorities and the geographic Commanders-in-Chiefs will demand more real time intelligence for strategic and tactical planning.<sup>29</sup> The present reactive stance of the community will have difficulty providing current intelligence on the broad and diverse spectrum of transnational issues and threats. This reactive stance is exacerbated by two problems. The first is the organization of the community itself, the second, the management of the huge amount of data generated by the various intelligence agencies.<sup>30</sup> Overlaid on

these two problem areas is this fourth dimension of cyberspace, the battleground of the future.<sup>31</sup>

Though the current legal paradigm of international and domestic law regarding armed conflict was developed over the past few centuries, this evolved set of legal principles allows, for the time being, a practitioner sufficient leeway upon which to operate in the fourth dimension of cyberspace.<sup>32</sup>

In short, the major hurdles regarding espionage and computer network attack are not legal, but organizational and technical. Some of the legal challenges revolve around intelligence oversight and the collection of intelligence on US persons, as well as the law of war. The intrusive nature of computers and the Internet and their use as tools of espionage, and even warfare, cause legal scholars and practitioners in national security some concern, not from the lack of precedent, but of policy.

### **The Current Domestic Legal Framework**

The current legal framework stems from statutory and regulatory guidance of the late 1970s, due to the improprieties by the US intelligence community in collecting information on US persons.<sup>33</sup> Centered on the National Security Act of 1947 and Executive Order 12333, intelligence organizations in the United States have been directed to follow certain prescribed procedures regarding the conduct of intelligence activities.<sup>34</sup>

The National Security Act of 1947, particularly Title V, gives authority for various departments and intelligence agencies to conduct intelligence gathering, laying out parameters as to what these organizations can or cannot do in the process.<sup>35</sup> One of the key statutory conditions is to keep the Congress currently and fully informed on all intelligence activities being conducted.<sup>36</sup>

Executive Order 12333, signed by President Reagan, lays out the various missions of the intelligence community and gives specific guidance on how to conduct intelligence activities.<sup>37</sup> Each department promulgates and expands on this guidance through departmental regulations.<sup>38</sup> Additionally, there are internal policy directives that further refine the methods by which the intelligence community can collect this intelligence.<sup>39</sup>

These rules, coupled with international law, allow the intelligence agencies to operate properly in cyberspace. If given the proper mission and authority, intelligence organizations can collect information (conduct espionage) in this fourth dimension. These operations can be done in peacetime, pre-hostilities (intelligence preparation of the battlefield), and during armed conflict.

The challenge is developing policy that allows the community to conduct espionage in cyberspace. Proper guidance is essential to ensure that sources and methods are not compromised, the operational environment is secure, proper counterintelligence concerns are addressed and monitored, and there is proper oversight to ensure that the civil rights of US persons are not violated.

### Some Policy Considerations

Operationally, cyberspace will pose the same challenges that a commander would face in a three-dimensional battle. Concepts of speed, mass, maneuver, surprise, taking the high ground, command and control, and forward support, among others, all apply in cyberspace. The Commander will need to be able to operate with as much familiarity and precision in this realm as he would on land, sea, or air—integrating all four dimensions seamlessly in achieving full spectrum dominance. He will also have to keep in mind, the four operational concepts espoused in the concept for future joint operations: dominant maneuver, precision engagement, full-dimensional protection, and focused logistics.<sup>40</sup>

Underlying all of the operational concepts listed above is the premise that new and emerging technologies will give joint US forces information superiority in any given mission. Information superiority is no longer a theory, but rather operational doctrine. Information superiority can be likened to the new high ground. A force that gains information dominance in the battlespace can shape it by making it not only more lethal for the adversary, but survivable for friendly forces.

A cornerstone in achieving this high ground is proper intelligence preparation of the battlespace itself using various methodologies, systems, and techniques to allow the commander to be dominant in his maneuver, precisely engaging the enemy in whatever dimension, supported by agile, innovative, focused personnel and organizations. Joint Publication 3-13, Joint Doctrine for Information Operations, describes intelligence preparation of the battlespace as “. . . the continuous process used to develop a detailed knowledge of the adversary system use of information and information systems.”<sup>41</sup>

The intelligence community’s challenge is to determine how far it can go to prepare that battlespace. Policy and operational concerns begin to surface as the transition takes place from a third dimensional conflict to operations in the fourth dimension of cyberspace. In attempting to understand the information environment, the operator will need knowledge of, *inter alia*, the adversary’s information systems; political, economic, social, and cultural makeup; decision making process; geographic strengths and weaknesses; and biographical/psychological profiles.<sup>42</sup>

Methods to achieve proper intelligence preparation of the battlespace could be intrusive, thereby butting up against privacy and oversight restrictions that could hamper and even impede the gathering of this intelligence. Intelligence oversight and review organizations will have to be aware of, and add within their training and review methodologies, information operations, to include principles of computer network attack and defense.

The potential for the inadvertent violation of civil rights of US persons is great due to the intrusive capabilities of these tools.<sup>43</sup> It must be noted, however, that these intrusive techniques have existed for many years and the oversight rules are generally sufficient to ensure proper operational use. The term “least intrusive means” is a standard in intelligence collection, similar to the proportionality concepts found in the law of armed conflict.<sup>44</sup>

As intelligence organizations plan and execute operations to prepare the battlespace, policy makers will have to determine how far the intelligence operator can go to prepare for any situation along the conflict spectrum. Misinterpretation by a potential adversary that this preparation could be indeed an attack requires careful planning and oversight to ensure that there is no inadvertent response by an aggrieved party on our information or economic infrastructure.

### **Concluding Thoughts . . .**

It is not constructive to change for change’s sake. Faced with new issues, the law moves slowly, but in most instances the lapse of time allows for the controversy to ripen and be properly resolved.<sup>45</sup> In the past this could take years. In this day and age, where a “web-year” of three months governs the business of the information market, the law could quickly become irrelevant and certainly a hindrance to both commerce and possibly our national security.

Practitioners must balance the need for a careful development of the law in the area of information operations with the fast-paced reality of the information age. The intelligence community itself, like the legal profession, also must develop a strategic plan akin to the vision of the Department of Defense in order to move steadily forward in improving organizational structures and developing more collaborative and streamlined information systems to support operations in cyberspace.

Where all this will end up is anyone’s guess. As in all things new, over-reactive quick fixes will in the long run cause more confusion and potential harm to this nation’s security. Additionally, treating information operations as a “different” operational tool for a commander in the field is a mistake. The doctrinal

and policy decisions by the Joint Staff to fully integrate information operations in operational planning are certainly steps in the right direction.

Operators and the legal community must continue to work for careful change domestically and provide leadership internationally to create appropriate rules in which future operations in cyberspace may be conducted within proper legal norms.

As former Secretary of Defense William Cohen declared:

If you can shut down our financial system, if you could shut down our transportation system, if you could cause the collapse of our energy production and distribution system just by typing on a computer and causing those links to this globalization to break down, then you're able to wage successful warfare and we have to be able to defend against that.<sup>46</sup>

---

### Notes

\* The views expressed in this paper are solely the author's and do not reflect the position of the Inspector General or the Department of Defense.

1. JAMES ADAMS, *THE NEXT WORLD WAR* 15 (1998).

2. David L. Grange, *Ready for What?*, *ARMED FORCES JOURNAL*, Dec. 1999, at 42. The article itself focuses mainly on the readiness reporting system and how it reflects readiness to meet the challenging new missions facing US Armed Forces. For an excellent discussion of future warfare and the challenges facing the US Army, see ROBERT H. ECCLES, *FUTURE WARFARE* (1999).

3. *See generally*, The United States Commission on National Security/21st Century, *New World Coming: American Security in the 21st Century (The Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century)*, Sept. 15, 1999. At page 7 the Commission states that the emerging security environment in the next quarter century will require different military and other national capabilities.

4. The Director of Central Intelligence, George Tenet, states in his (U)Strategic Intent for the Intelligence Community (S/NF) that "success in the 21st Century will require closer cooperation and more efficient use of our capabilities" (at 1).

5. There is an interesting development in the way nations/peoples prepare to fight technologically. The Tofflers in their book *WAR AND ANTI-WAR*, place these various methodologies in waves. Their premise is that throughout history man wages war the way he works. Consisting of three waves, the first wave centered around agriculture, the second wave on the industrial revolution, and the third on knowledge and information. Each had a profound affect on the way war was waged. *See generally*, ALVIN AND HEIDI TOFFLER, *WAR AND ANTI-WAR* (1993). Today all three waves exist simultaneously, a phenomenon generally not encountered in the past. For instance, in Somalia, information warriors have faced and have been challenged by agricultural workers fighting with spear and shield. This imbalance caused these highly technical soldiers to fight the Somalis on their terms, as technology/information operations proved ineffective against these first wave warriors. *See also* ROBERT W. CHANDLER, *NEW FACE OF WAR* (1998), which focuses on the impact of weapons of mass destruction and America's military strategy.

6. Espionage falls within the parameters of the inherent right of self-defense and is also lawful under the law of armed conflict. *See* NATIONAL SECURITY LAW 443 (John N. Moore et al., eds.

1990); Hague Convention IV Respecting the Law and Customs of War on Land, Oct. 18, 1907, Annex (Regulations), arts. 24, 29–31, 36 Stat. 2295, 1 Bevans 643.

7. JOHN P. FINNEGAN, *THE MILITARY INTELLIGENCE STORY*, at V (1994). See generally, GEORGE O'TOOLE, *HONORABLE TREACHERY*, (1991). In *POWER SHIFT* (1991), Alvin Toffler declares at page 289 that “Spies have been busily at work at least since the Egyptian Book of the Dead termed espionage a soul-endangering sin.”

8. *WAR AND ANTI-WAR*, *supra* note 5, at 154. See also William Clinton, *A NATIONAL SECURITY STRATEGY FOR A NEW CENTURY* 24 (1998) and *COMBATING PROLIFERATION OF WEAPONS OF MASS DESTRUCTION*, Report from the Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction (1999), at 66.

9. See *THE MILITARY INTELLIGENCE STORY*, *supra* note 8, at 19. See also *HONORABLE TREACHERY* *supra* note 7, at 492–493; DAVID MURPHY ET AL., *BATTLEGROUND BERLIN*, at ix, 398 (1997).

10. The National Command Authorities (NCA) consist of the President and the Secretary of Defense collectively. See generally, 10 US Code § 162(b). The NCA is different than the National Security Council (NSC), created by the 1947 National Security Act, 50 US Code § 40. The NSC membership consists of the President, Vice President, Secretary of Defense, and the Secretary of State. Statutory advisors are the Chairman of the Joint Chiefs of Staff and the Director of Central Intelligence.

11. The intelligence community is composed of 13 agencies, including those in the Departments of Defense, Justice, Treasury, Energy, and State, as well as the Central Intelligence Agency (CIA). See *OFFICE OF PUBLIC AFFAIRS, CIA, A CONSUMER'S GUIDE TO INTELLIGENCE*, at vii and 28 (1999). The majority of assets and organizations are in the Department of Defense. These include the Defense Intelligence Agency, the National Imagery and Mapping Agency, the National Reconnaissance Office, and the National Security Agency, among others. The missions of the various agencies and intelligence components within the US intelligence community can generally be found in E.O. 12333, *US Intelligence Activities*, (December 4, 1981, 46 Federal Register 59941).

12. In *WAR AND ANTI-WAR*, *supra* note 5, at 154 the Tofflers state:

Among all the “national security” institutions, none have a deeper need for restructure and reconceptualization than those devoted to foreign intelligence. Intelligence, as we’ve seen, is an essential component of any military knowledge strategy. But as the Third Wave war-form takes shape, either intelligence itself assumes a Third Wave form, meaning it reflects the new role of information, communication, and knowledge in society, or it becomes costly, irrelevant, or dangerously misleading.

See also *THE NEXT WORLD WAR*, *supra* note 1, at 258. Adams writes:

As with so many things, the end of the Cold War and the advent of the Information Age caused a seismic shift in the world of espionage. Spy agencies needed a reason to be; although the need for intelligence had not lessened, the fact that most required knowledge was rapidly becoming available on the Internet meant that cloak and dagger was beginning to take second place to the drudge of reading and analyzing mountains of online reports.

13. See generally, *VENONA: SOVIET ESPIONAGE AND THE AMERICAN RESPONSE 1939–1957* (Robert Benson and Michael Warner eds., 1996); *THE MILITARY INTELLIGENCE STORY*, *supra* note 7; *HONORABLE TREACHERY*, *supra* note 7; SHERRY SONTAG AND CHRISTOPHER DREW, *BLIND MAN'S BLUFF* (1998).

14. There are five basic intelligence sources, or collection disciplines: Signals Intelligence (SIGINT) includes information derived from intercepted communications, radar, and telemetry; Human-source Intelligence (HUMINT) derived information from both clandestine and overt

collections techniques; Imagery Intelligence (IMINT) which provides information from overhead and ground imagery; and Measurement and Signatures Intelligence (MASINT) is that information that comes from technical means other than imagery or SIGINT. A CONSUMER'S GUIDE TO INTELLIGENCE, *supra* note 11, at 2.

15. The Tofflers declare that "The Shift to a Third Wave intelligence system, paradoxically, means a stronger emphasis on human spies. . . ." WAR AND ANTI-WAR, *supra* note 5, at 158. They go on to say that "the Third Wave explosion of information and communication means that more and more of what decision makers need to know can be found in 'open' sources." *Id.* at 160. OSINT is information that is publicly available, as well as other unclassified information that has limited public distribution or access. Open source information also includes any information that may be used in an unclassified context without compromising national security or intelligence sources or methods.

16. WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 124-125 (1999).

17. NATIONAL SECURITY LAW, *supra* note 6, at 438-42; Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations, at I-9 & I-10 (1998) [hereinafter Joint Pub 3-13].

18. GEORGE CONSTANTINIDES, INTELLIGENCE AND ESPIONAGE 11 (1983).

19. HENRY L. STIMSON AND MCGEORGE BUNDY, ON ACTIVE SERVICE IN PEACE AND WAR 188 (1948). As Secretary of State, Stimson shut down the State Department's code breaking unit in 1929, remarking ". . . that gentlemen do not read other people's mail." See also HONORABLE TREACHERY, *supra* note 7, at 3. O'Toole asserts: "American gentlemen have read other people's mail at every major turning of our national career. What is more, American gentlemen have proved to be very good at it." *Id.* at 3. President Harry Truman is attributed to have said during the signing of the National Security Act of 1947 that "intelligence and a free society do not mix."

20. Henry James captured the American attitude when he stated:

American innocence contrasted with European subtlety and corruption. Americans are blunt, forthright, direct, ingenuous—all qualities acquired on the frontier and permanently incorporated in the American national character. Deviousness, secretiveness, indirection, and duplicity are, literally, foreign.

HONORABLE TREACHERY, *supra* note 7, at 3. Robert Gates, a former Director of Central Intelligence, writes:

Presidents expect that, for what they spend on intelligence, the product should be able to predict coups, upheavals, riots, intentions, military moves, and the like with accuracy. . . . Presidents and their national security teams usually are ill-informed about intelligence capabilities; therefore they often have unrealistic expectations of what intelligence can do for them, especially when they hear about the genuinely extraordinary capabilities of U.S. intelligence for collecting and processing information.

Robert Gates, *An Opportunity Unfulfilled: The Use and Perceptions of Intelligence at the White House*, WASHINGTON QUARTERLY, Winter 1989, at 38-39.

21. See generally, THE MILITARY INTELLIGENCE STORY, *supra* note 7; HONORABLE TREACHERY, *supra* note 7; CHRISTOPHER M. ANDREW, FOR THE PRESIDENT'S EYES ONLY (1995).

22. Regarding the state of counterespionage in the US around the time of the First World War, Christopher Andrew states:

No nation was less ready than the United States. Neither the Justice Department's Bureau of Investigation (the future FBI) nor the Treasury Department's Secret Service had much experience of counterespionage work. Each made matters worse by refusing to cooperate with the other.

FOR THE PRESIDENT'S EYES ONLY, *supra* note 21 at 30.

23. See generally, THE MILITARY INTELLIGENCE STORY, *supra* note 7; DAVID CRANE, COUNTERINTELLIGENCE COORDINATION (1995).

24. In 1966, Senator Daniel K. Inouye (Democrat, Hawaii), the first Chairman of the Senate Select Committee on Intelligence, declared:

I recall when we came to classified programs, we would all look over at Richard Russell, the Chairman of the Armed Services Committee, and he would say, "I have discussed this matter with the appropriate officials and I have found everything is in order. . . ." But no one ever told us what was in order.

HONORABLE TREACHERY, *supra* note 7.

25. See Preparing for the 21st Century, An Appraisal of U.S. Intelligence, Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, March 1, 1996, at A-14.

26. These committees are: The Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Both of these committees (generally known as the Intelligence Committees) were established in 1976.

27. HONORABLE TREACHERY, *supra* note 7, at 427. It is interesting to note that President Truman initially gave the job of creating a centralized organization to the Secretary of State, James Byrnes, who promptly tabled the idea where it languished for over a year. See also, FOR THE PRESIDENT'S EYES ONLY, *supra* note 21, at 149.

28. See generally, Joint Pub 3-13, *supra* note 17, at II-11. The Joint Staff pointedly declares that "offensive IO [information operations] require broad-based, dedicated intelligence support. Because intelligence support to offensive IO may require significant lead time and the effectiveness of many offensive capabilities is significantly improved by early employment, potential intelligence collection sources and access should be developed as early as possible." Computer network attack is defined in the same publication as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA." *Id.* at glossary.

29. The combatant commands are statutorily created. 10 US Code § 161(a). Currently, there are nine combatant commands, five with geographic responsibility, e.g., Southern Command (SOUTHCOM), and four with functional responsibilities, e.g., Space Command (SPACECOM). 10 US Code § 164 lists the powers of a combatant commander who exercises combatant command (COCOM). See Chairman of the Joint Chiefs of Staff, Joint Publication 0-2, Unified Action Armed Forces (1995). The combatant commands are commonly referred to as the "warfighters." For an excellent overall summation of the roles and responsibilities of the NSC, NCA, and the combatant commands, see THE ARMY JUDGE ADVOCATE GENERAL'S SCHOOL, OPERATIONAL LAW HANDBOOK, Ch. 2, (2000).

30. NIMA Infotech Retools U.S. Space Recon Ops, AVIATION WEEK & SPACE TECHNOLOGY, Aug. 7, 2000, at 62.

31. Joint Vision 2010 states that information superiority is a key force multiplier and operational capability in future battlespace, providing full spectrum dominance to shape the strategic environment. See JOINT WARFIGHTER CENTER, CONCEPT FOR FUTURE JOINT OPERATIONS 35-36 (1997).

32. A concern is the attempt to create new rules for new technologies and ideas, without a proper understanding or consideration for the basic principles of international law and the law of armed conflict. Practitioners in the field of operational law in the armed services understand that in general the current legal regime allows for the proper conduct of information operations.

33. See Seymour M. Hersch, *Huge CIA Operations Reported in US Against Antiwar Forces*, NEW YORK TIMES, Dec. 22, 1974, at A1; The Evolution of the US Intelligence Community—An

Historical Overview, in Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, at A-14 (1996).

34. E.O. No. 12333, *supra* note 11. In the introduction to E.O. 12333, President Reagan directs:

Timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons, and their agents is essential to the national security of the United States. All reasonable and lawful means must be used to ensure that the United States will receive the best intelligence available.

35. 50 US Code 401 *et seq.* (cited as “National Security Act of 1947”). The preamble to the original act of July 26, 1947, declares:

AN ACT to promote the national security by providing for a Secretary of Defense; for a National Military Establishment; for a Department of the Army, a Department of the Navy, and a Department of the Air Force; and for the coordination of the activities of the National Military Establishment with other departments and agencies of the Government concerned with the national security.

36. 50 US Code § 501.

37. Sect. 1.12, E.O. 12333, *supra* note 11.

38. The Department of Defense has published this guidance in DoD Directive 5240.1, DoD Intelligence Activities (Apr. 25, 1988); DoD Directive 5240.1R, Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons (July 1, 1982).

39. *See generally*, for example, Department of the Army Regulation 381-10, US Army Intelligence Activities (July 1, 1984), and Defense Intelligence Agency, Intelligence Law Handbook (Sept. 1995).

40. CONCEPT FOR FUTURE JOINT OPERATIONS, *supra* note 31, at Introduction.

41. Joint Pub. 3-13, *supra* note 17, at II-12. *See also* Chairman of the Joint Chiefs of Staff, Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace (2000).

42. *Id.* at II-12-13.

43. A US person is defined as:

... a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

E.O. 12333, *supra* note 11, at para. 3.4.

44. For the principle of proportionality, *see generally*, US Army Field Manual 27-10, THE LAW OF LAND WARFARE at para. 41 (1956). Generally, the test is that the loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained. OPERATIONAL LAW HANDBOOK, *supra* note 29, at 7-4. Compare with the rule of least intrusive means found in E.O. 12333, *supra* note 11, at pt. 2.4 (implemented in DoD Directive 5240.1-R, *supra* note 38, Procedure 1, Sect. A.4, and Procedure 2, Sect. D), which states that the collection of information by a DoD intelligence component must be accomplished by the least intrusive means or lawful investigative technique reasonably available.

45. As Sophocles declared in *Oedipus Rex*, “Time eases all things.”

46. Speech to the Veterans of Foreign Wars and the Ladies Auxiliary, reported in FEDERAL COMPUTER WEEK, Aug. 28, 2000.