Congressional Research Service
Informing the legislative debate since 1914

Information Warfare: Issues for Congress

Catherine A. Theohary
Specialist in National Security Policy, Cyber and Information Operations

March 5, 2018

Congressional Research Service
7-5700
www.crs.gov
R45142

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Information warfare is hardly a new endeavor. In the Battle of Thermopylae in 480 BC, Persian ruler Xerxes used intimidation tactics to break the will of Greek city-states. Alexander the Great used cultural assimilation to subdue dissent and maintain conquered lands. Military scholars trace the modern use of information as a tool in guerilla warfare to fifth-century BC Chinese military strategist Sun Tzu's book *The Art of War* and its emphasis on accurate intelligence for decision superiority over a mightier foe. These ancient strategists helped to lay the foundation for information warfare strategy in modern times.

Taking place below the level of armed conflict, information warfare (IW) is the range of military and government operations to protect and exploit the information environment. Although information is recognized as an element of national power, IW is a relatively poorly understood concept in the United States, with several other terms being used to describe the same or similar sets of activity. IW is a strategy for using information to pursue a competitive advantage, including offensive and defensive efforts. A form of political warfare, IW is a means through which nations achieve strategic objectives and advance foreign policy goals. Defensive efforts include information assurance/information security, while offensive efforts include information operations. Similar terms sometimes used to characterize information warfare include active measures, hybrid warfare, and gray zone warfare.

IW is sometimes referred to as a "disinformation campaign," yet disinformation is only one of the tactics used in information operations (IO). The types of information used in IO include propaganda, misinformation, and disinformation.

As cyberspace presents an easy, cost-effective method to communicate a message to large swaths of populations, much of present day information warfare takes place on the internet, leading some to conflate "cyberwarfare" with information warfare. While IO in the United States tends to be seen as a purely military activity, other countries and terrorist organizations have robust information warfare strategies and use a whole-of-government or whole-of-society approach to information operations.

In terms of U.S. government bureaucracy, there are debates in the United States about where the IW center of gravity should be. During the Cold War, the epicenter in the U.S. government was the Department of State and the U.S. Information Agency. Since 9/11, much of the current doctrine and capability resides with the military, leading some to posit that the epicenter should be the Pentagon. But others worry that the military should not be involved in the production of propaganda.

This report offers Congress a conceptual framework for understanding IW as a strategy, discusses past and present IW-related organizations within the U.S. government, and uses several case studies as examples of IW strategy in practice. Countries discussed include Russia, China, North Korea, and Iran. The Islamic State is also discussed.

Contents

Contacts

Introduction: What Is Information Warfare?

Information warfare (IW) is a term that appears in recent hearings, news articles, and government documents. Yet these same documents may use other terms to describe the same sets of activities or concepts. As the definition can affect how the government strategizes, organizes, trains, and equips around that term, Congress may be interested in pursuing a definitive theory of IW.

While there is currently no official U.S. government definition of IW, it is typically conceptualized as the use and management of information to pursue a competitive advantage, including offensive and defensive efforts. For some in the United States, the term "warfare" implies armed conflict or other military activity; yet political warfare is commonly understood as the use of political means to compel an opponent to do one's will. According to Cold War diplomat George Kennan's definition, political warfare is the

> employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures, and "white" propaganda to such covert operations as clandestine support of 'friendly' foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[1]

In this sense, IW is a form of political warfare, where targets include a nation state's government, military, private sector, and general population.

Taking place below the level of armed conflict, IW is the range of military and government operations to protect and exploit the information environment. It consists of both offensive and defensive operations: the protection and assurance of one's own information (information security), and information operations to advance interests. It is conducted not only in crisis, conflict, and warfare in the operational sense, but is ongoing in peacetime as well. Whether attacking government agencies, political leadership, or news media in order to influence public opinion or to compel decisionmakers to take certain actions, ultimately the target of information warfare activities is human cognition. For this reason, information warfare is sometimes referred to as persuasion or influence operations, or even psychological operations.

Yet information warfare may not always involve compelling or coercing decisions; rather, it may be part of a "divide and conquer"[2] strategy targeting civil society, sowing confusion in a target population in order to create decision paralysis. Decisionmakers in this case are constantly bombarded by contradictory reports, with no readily available means of discerning the truth. In the absence of reliable information and facing heightened opposition from factions on both sides of an issue, decisionmakers may be unable to act. This is the informational equivalent of what Carl von Clausewitz coined as the "fog and friction" of war.[3] The fog of war refers to the uncertainty in situational awareness experienced by participants in military operations, while friction is a by-product of this fog.

IW is a whole-of-society endeavor, in which civilians may be knowingly or unknowingly functioning as proxies on behalf of a government. For example, the Russian concept of IW describes preemptive operations to achieve political goals and to control the information space,

[1] Kennan, George F., "On Organizing Political Warfare," National Security Council Policy Planning Staff document, April 30, 1948.

[2] "Divide and conquer" refers to the policy of maintaining control by encouraging infighting and dissent among concentrations of power.

[3] Von Clausewitz, Carl, *On War*, Princeton University Press, June 1, 1989.

deploying all elements of society to include patriotic hacker groups and private citizens.[4] The Chinese theory of IW is integrated into "The People's War"[5] concept and involves the use of information technologies by hundreds of millions of people in order to influence an adversary's policymakers, and to gain an advantage against an asymmetric threat. Authoritarian regimes and their control over information infrastructure facilitate the use of a wide range of actors and techniques. These regimes may compel ordinary citizens to act as agents of information warfare with financial rewards, by appealing to a sense of patriotism, or through threats and coercion.

Information warfare may be a prelude to an armed conflict, a preparation of the battlefield preceding the deployment of forces. Information operations set the conditions in theater to gain support of locals, "winning the hearts and minds"[6] to increase the odds of a successful campaign. Alternatively, IW may be an end in and of itself, the process through which nations gain competitive advantages over one another without the use of force.

There may be many terms that describe the use of information as a weapon. However, because of its emphasis on the strategic implications of mobilizing information as an instrument of power, information warfare is a useful term to describe this particular strategy.

Information Warfare Strategy vs. Information Operations

Modern military theory, going back as far as the Napoleonic era, divides warfare into three levels: strategic, operational, and tactical. Strategy can be defined as the process of planning to achieve objective and goals in the national interest. For the military, this typically involves identification of the ends, ways, and means of achievement of stated goals. The Department of Defense (DOD) Dictionary of Military and Associated Terms defines the strategic level of warfare as the level at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives.[7] Information warfare takes place at the strategic level, while information operations (IO) involve using various information-related capabilities to implement the strategy. The operational level is that at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas.[8] Operations link these strategic objectives with specific tactics, techniques, and procedures in order to achieve them. The tactical level of warfare concerns the ordered arrangement and maneuver of combat elements in relation to each other and the enemy to achieve combat objectives. IO happens at the operational level, linking information-related capabilities and tactics to a broader strategy.

[4] For a discussion of Russian IW strategy, see Statement of Timothy Thomas before the House Armed Services Subcommittee on Emerging Threats and Capabilities, March 15, 2017, http://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf.

[5] The people's war is a strategy developed by Mao Zedong, the goal of which is to maintain support of the population and defeat the enemy through conventional and guerilla warfare. See Mao's "On Protracted War," May 1938.

[6] Winning hearts and minds refers to the U.S. strategy in the Vietnam War to win the popular support of the Vietnamese people to help defeat the Viet Cong insurgency.

[7] DOD Dictionary of Military and Associated Terms, available at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

[8] Ibid.

Information Operations

Current and past U.S. government definitions have conceptualized information operations as a purely military activity involving a set of tactics or capabilities. In an earlier version of DOD's Joint Publication 3-13 and the Information Operations Roadmap, IO consisted of five pillars:

- computer network operations (CNO), which consisted of
    - computer network attack (CNA)
    - computer network defense (CND)
    - computer network exploitation (CNE),
- psychological operations (PSYOP),
- electronic warfare,
- operations security (OPSEC), and
- military deception (MILDEC).[9]

CNO later became cyberspace operations, offensive and defensive, with its own separate doctrine in Joint Publication 3-12.[10]

Psychological operations involve the planned use of information (propaganda) to influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. At the strategic level, PSYOPs are the delivery of information to influence foreign target audiences in support of U.S. goals and objectives. PSYOPs at the operational level are conducted in support of the combatant commander's mission accomplishment, either independently or as an integral part of other operations. Previous definitions of psychological operations resemble what some term as information operations or information warfare. In later doctrine, PSYOP was changed to military information support operations (MISO).

Electronic warfare is defined as military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Examples include jamming command and control systems, satellites used for global positioning systems, and radio communications.

Operations security is the process of identifying critical information and analyzing friendly actions attendant to military operations and other activities.

Military deception is actions to deliberately mislead adversary military, paramilitary, or violent extremist organization decisionmakers, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. A pillar closely related to PSYOP, MILDEC focuses on false information or disinformation.

The Secretary of Defense now characterizes IO in JP 3-13[11] as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own." This definition shifts the focus from a set of tactics or

[9] Declassified in 2006, the Department of Defense Information Roadmap is available in a redacted version at https://nsarchive2.gwu.edu/NSAEBB/NSAEBB177/info_ops_roadmap.pdf.

[10] Joint Chiefs of Staff, Joint Publication 3-12 (R) Cyberspace Operations, February 5, 2013.

[11] Joint Chiefs of Staff, Joint Publication 3-13 Information Operations, November 27, 2012.

pillars toward the desired effects and how to achieve them. JP3-13 defines information-related capability as a tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions. Strategic communication, public diplomacy, public and civil affairs, and cyberspace operations may be considered supporting capabilities. They may take place outside of cyberspace, such as dropping pamphlets, cultural exchanges, civil affairs, and foreign aid programs to gain favor with a target population.

Under the current definition, a primary component of IO is MISO (formerly PSYOP), which are planned operations to convey selected information and indicators to foreign audiences to influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. MISO focuses on the cognitive element of the information environment where its target audience includes not just potential and actual adversaries, but also friendly and neutral populations.

Some entities within the U.S. military are returning to the PSYOP title, possibly in hopes of regaining the esprit de corps formerly associated with the name. For example, the Army recently announced its intent to rename its units from MISO to PSYOP.[12]

Information Warfare-Related Terms

National security strategists may use other terms to describe information warfare. These terms tend to focus on either the military or government application of information and can miss the various information-related capabilities that embody IW as a whole. Several other related terms are often used in conjunction with IW as they convey similar concepts.

Active measures are activities undertaken to achieve foreign policy objectives by state-sponsored influence operations targeting citizenry, influence operations between nations, and population-to-population influence operations.[13]

Hybrid warfare blends conventional, irregular, and information warfare. It may also include economic and other forms of competition and contention. Often used to describe information warfare, hybrid warfare encompasses activities that fall outside of the information warfare rubric.

Gray zone warfare entails techniques to achieve a nation's goals while denying those of its rivals by employing instruments of power that do not necessarily include use of acknowledged regular military forces. These may involve state and nonstate actors, and fall between traditional wars and peacetime.

Irregular warfare is a "violent struggle among state and non-state actors for legitimacy and influence over the relevant populations."[14] It is also known as tribal warfare or low-intensity conflict, often characterized by the absence of traditional military entities.

[12] Myers, Meghann, "The Army's Psychological Operations Community is Getting its Name Back," *Army Times,* November 6, 2017, https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/.

[13] A 1988 report of the U.S. Information Agency refers to the Soviet term "active measures" as a form of political warfare with deceptive and manipulative elements. See Abrams, Steve, "Beyond Propaganda: Soviet Active Measures in Putin's Russia," *Connections: The Quarterly Journal,* Winter 2016.

[14] Department of Defense, "Irregular Warfare Joint Operating Concept," Version 1.0, February 27, 2009.

Unconventional warfare is the support of a foreign insurgency against its government or occupying power. It relies heavily on subversion through information and guerilla warfare, and forces are often covert.

Asymmetric warfare is fought between belligerents whose relative military power or whose strategy or tactics differ significantly. Information warfare can be a successful means of overcoming the disparity.

Soft power is, according to international relations scholar Joseph Nye, "the ability to get what you want through attraction rather than coercion or payments." This may involve the use of information with a positive spin in order to compel decisionmakers toward actions in one's own interests.

Public diplomacy refers to government-sponsored programs intended to inform or influence public opinion in other countries; its chief instruments are publications, motion pictures, cultural exchanges, radio, and television.[15]

Types of Information

In common parlance, the term "disinformation campaign" is often used interchangeably with information operations. However, disinformation or deception is only one of the informational tools that can be exploited as part of an IW strategy; factual information can also be used to achieve strategic goals and in some cases more effectively than deceptive means. Different categories of information may be used in IO, including the following:

Propaganda: This is the propagation of an idea or narrative that is intended to influence, similar to psychological or influence operations. It can be misleading but true, and may include stolen information. A government communicating its intent, policies, and values through speeches, press releases, and other public affairs can be considered propaganda as well as public diplomacy. These communications have strategic value in that over time they can create perceptions that steer decisionmakers towards a certain course of action.

Misinformation: This is the spreading of unintentionally false information. Examples include internet trolls who spread unfounded conspiracy theories or web hoaxes through social media, believing them to be true. Misinformation can have the effect of sowing divisiveness and chaos in a target society, as the truth becomes harder to discern.

Disinformation: Unlike misinformation, disinformation is intentionally false. Examples include planting deliberately false news stories in the media, manufacturing protests, doctoring pictures, and tampering with private and/or classified communications before their widespread release.

All of these activities take place within the information environment,[16] which is the aggregate of individuals, organizations, and systems that collect, disseminate, or act on information. This includes

- **The physical layer:** Command and control systems and associated infrastructure.
- **The informational layer:** Networks and systems where information is stored.
- **The cognitive layer:** The minds of people who transmit and respond to information.

[15] This definition is from the U.S. Department of State Dictionary of International Relations Terms, Reprints from the collection of the University of Michigan Library, January 1, 1987.

[16] JP 3-13.

All instruments of national power—diplomatic, informational, military, and economic (DIME)—can be projected and employed in the information environment.

Information Operations in Cyberspace

William Gibson coined the term cyberspace in his 1984 novel, *Neuromancer*, as a "consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts.... A graphic representation of data abstracted from the banks of every computer in the human system."[17] This definition emphasizes the human element, with cyberspace as something that exists in people's minds.

In JP 3-12, DOD defines cyberspace as "the global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[18] Some have criticized this as lacking the cognitive, human element that the internet represents, which in turn could adversely affect how the military organizes, trains, and equips for IO.

Cyberspace presents a force multiplier for IW activities. Social media and botnets can amplify a message or narrative, using all three elements of information to foment discord and confusion in a target audience.[19] Much of today's IW is conducted in cyberspace, leading many to associate IO with cybersecurity. Within DOD, however, IO and cyberspace operations are distinct doctrinal activities. Cyberspace operations can be used to achieve strategic information warfare goals; an offensive cyberattack, for example, may be used to create psychological effects in a target population. A foreign country may use cyberattacks to influence decisionmaking and change behaviors, for example the Democratic People's Republic of Korea (DPRK)-attributed cyberattacks on Sony in late 2014. Cyber operations may be conducted for other purposes, such as to disable or deny access to an adversary's lines of communication, or to degrade components of critical infrastructure that may be used for nefarious purposes.[20]

IO may be overt, such as a government's production and dissemination of materials intended to convey democratic values. In this case, the government sponsorship of such activity is known. Covert operations are those in which government sponsorship is denied if exposed. The anonymity afforded by cyberspace can present an ideal battle space to conduct covert information operations. In addition, IO may take place outside of cyberspace.

Although several official documents now refer to "information warfare" in other countries, the United States has no formal government definition of IW. The DOD definition of information operations refers only to military operations and does not emphasize the use of cyberspace to achieve nonmilitary strategic objectives. Similarly, there is no commonly accepted definition of "cyberwarfare"; rather, the military refers to offensive and defensive cyberspace operations, with cyberspace as a warfighting domain or operating environment.

Cyberspace operations differ from information operations, which are specifically concerned with the use of information-related capabilities, such as military information support operations or

[17] Gibson, William, *Neuromancer*, Ace Books: New York, July 1, 1984.

[18] Department of Defense, Joint Publication 3-12, Cyberspace Operations.

[19] A botnet is a group of computers that have been infected with malicious software, allowing them to be controlled and used without the owners' knowledge.

[20] For example, a critical infrastructure platform may be used to conduct cybercrime for fundraising efforts or to launch debilitating cyberattacks on an adversary.

military deception. Cyber-enabled information operations can be characterized as IO conducted in cyberspace. Just as IO carries its own doctrine and associated organizational structures, so do cyberspace operations, which are generally considered the purview of the United States Cyber Command.

The U.S. Cyber Command is building a national cyber mission force composed of three teams, one of which assists combatant commanders in the field with planning and operations. These teams may, for example, target and dismantle violent extremist websites that present an operational threat to troops on the ground. However, this cyber force is structurally and conceptually separated from the troops responsible for conducting information operations. As previously stated, the two forces operate under separate doctrine. The two are physically separated as well: U.S. Cyber Command is located in Fort Meade, MD, while the Joint Information Operations Warfare Center is located at Lackland Air Force Base, Texas.

Who Is Responsible for the "I" in DIME?

As a source of national power, information is a critical strategic asset, and currently the information element is shared within the U.S. government.[21] During the Cold War, the U.S. Information Agency (USIA) was responsible for supporting U.S. national interests abroad through information dissemination. It was later folded into the State Department's Bureau of Public Diplomacy and Public Affairs before being disbanded in 1999. Today, the Department of State-led interagency Global Engagement Center (GEC) is charged with many of the former USIA activities. According to Steve Goldstein, then Undersecretary for Public Diplomacy, the GEC recently launched a new $40 million initiative to battle state-sponsored disinformation and propaganda targeting the United States and its interests.[22] It also plans to launch a series of pilot projects with the Department of Defense, using additional DOD funding.

Within the U.S. government, much of the current information warfare doctrine and capability resides with the military, making it the de facto center of gravity.[23] DOD is also relatively well-funded, leading some to posit that the epicenter for IW activities should be the Pentagon. Some fear that military leadership of the IW sphere represents the militarization of cyberspace, or the weaponization of information that would counter the principles of global internet freedom. Title 10 U.S.C 2241 prohibits DOD from domestic "publicity or propaganda," although the terms are undefined. It is unclear how IW/IO relate to this so-called military propaganda ban.

The Central Intelligence Agency (CIA) has a history of conducting information warfare or psychological operations, particularly with respect to countering guerilla organizations abroad. Monitoring Soviet disinformation was once solely the purview of the CIA, until the Active Measures Working Group was established in 1981 and tasked with coordinating the activities of multiple, disparate activities within the U.S. government.

[21] Within the national security community, the DIME decisionmaking model is a categorization of actions based on aspects of national power. Each categorization—Diplomatic, Informational, Military, and Economic—is an instrument of national power

[22] Department of State, Office of the Spokesperson, "State-Defense Cooperation on Global Engagement Center Programs and Creation of the Information Access Fund to Counter State-Sponsored Disinformation," February 26, 2018.

[23] Originating with Clausewitz, the center of gravity concept is defined by the DOD as "the source of power that provides moral or physical strength, freedom of action, or will to act." DOD, "Dictionary of Military and Associated Terms," February, 2018, at http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf.

During the Cold War, the Interagency Active Measures Working Group collected and analyzed information gathered at USIA overseas posts, from CIA reporting, and FBI investigations in order to detect and expose Soviet propaganda and disinformation efforts. This information was published in publicly disseminated reports. The final report of the Active Measures Working Group in 1992 warned that with the dissolution of the Soviet Union, active measures remained a threat to U.S. interests: "As long as states and groups interested in manipulating world opinion, limiting U.S. government actions, or generating opposition to U.S. policies and interests continue to use these techniques, there will be a need for the United States Information Agency to systematically monitor, analyze, and counter them."[24] Because there is no similar entity existing today, some government analysts have suggested that a version of the Active Measures Working Group be convened to face the current threat environment. Similarly, there have been calls for the resurrection of the U.S. Information Agency, but with added responsibilities.

Case Studies: IW in Practice

Information warfare is hardly a new endeavor. In the Battle of Thermopylae in 480 BC, Persian ruler Xerxes used intimidation tactics to break the will of Greek city-states. Alexander the Great used cultural assimilation to subdue dissent and maintain conquered lands. These ancient strategists helped to lay the foundation for information warfare strategy in modern times.

Information and Guerilla Warfare

Information warfare can be an effective means of fighting a guerilla war, a form of irregular warfare in which small groups of combatants take actions against local military, police forces, and rival insurgent forces. For example, information operations, both PSYOP and MILDEC, played a prominent role on both sides of the Hukbalahap Rebellion, an extended guerilla war that began in 1942 in the Philippines and ended in 1954. First, Huk rebels promoted the narrative of themselves as benevolent saviors of the locals and the Philippine government as the enemy. Later, with the advice of U.S. Air Force Major General Edward Lansdale, the Armed Forces of the Philippines conducted information operations to counter this message and in particular used military deception tactics to confuse and entrap the rebels.[25] In Nicaragua in the 1980s, the CIA wrote a manual on psychological operations for the contras for use in their civil war against the Nicaraguan government.[26] The manual described "selective use of violence for propagandistic effects," and to neutralize government officials. In particular, the manual recommended that the Contras lure demonstrators into clashes with authorities to provoke riots or shootings that could be used to further enflame public sentiment against the government.

Some scholars cite the American Revolutionary war as an example of PSYOP and guerilla warfare tactics. During this conflict, American forces distributed leaflets that negatively portrayed the conditions in British camps in order to demoralize their troops. Leaflets also promised British troops free land if they defected to the American side.[27]

[24] Department of State, "Soviet Influence Activities: A Report on Active Measures and Propaganda, 1987-1988," August 1989.

[25] For more information, see Lansdale, Edward, *In the Midst of Wars*, Fordham University Press, January 1, 1991.

[26] Tayacan, "Psychological Operation in Guerilla Warfare," October 18, 1984, https://www.cia.gov/library/readingroom/docs/CIA-RDP86M00886R001300010029-9.pdf

[27] For a survey of such operations throughout history, see Curtis, Glenn, "An Overview of Psychological Operations (PSYOP)," Library of Congress Federal Research Division, October 1989, at http://www.dtic.mil/get-tr-doc/pdf?AD=

(continued...)

Military scholars trace the modern use of information as a tool in guerilla warfare to fifth-century BC Chinese military strategist Sun Tzu's book *The Art of War* and its emphasis on accurate intelligence for decision superiority over a mightier foe.[28]

Nation States and Terrorist Organizations

Both nation states and terrorist organizations pursue information warfare to achieve strategic objectives. The following examples highlight the ways in which their IW strategies may already be in effect. These threats are prioritized in the recent National Defense Strategy, which refers specifically to information warfare as a means through which "competitors and adversaries seek to optimize their targeting of our battle networks and operational concepts, while also using other areas of competition short of open warfare to achieve their ends."[29]

Russia

Russia is engaging in activities that it describes in doctrine as information warfare. A 2011 Russian strategy document, the Convention on International Information Security, defines IW as "a conflict between two or more States in the information space[30] with the goal of inflicting damage to information systems as well as carrying out mass psychological campaigns against the population of a State in order to destabilize society and the government; as well as forcing a State to make decisions in the interests of their opponents."[31] An "information weapon" is information technology, means, and methods intended for use in information warfare. Russian doctrine typically refers to a holistic concept of "information war," which is used to accomplish two primary aims:

- to achieve political objectives without the use of military force, and
- to shape a favorable international response to the deployment of its military forces, or military forces with which Moscow is allied.

To accomplish these goals, Russia appears to be using social media tools to spread a mix of propaganda, misinformation, and deliberately misleading or corrupted disinformation. Tactics also include data breaches of servers of U.S. political parties and other groups, releases and possible manipulation of sensitive documents in an attempt to influence the U.S. presidential election, and the manipulation of publicly available information on Russian activities in Ukraine.

On January 6, 2017, the Office of the Director of National Intelligence (ODNI) released a declassified report on Russian activities and intentions related to the 2016 U.S. presidential

(...continued)

ADA302389.

[28] See Griffith, Samuel B., *The Illustrated Art of War*, Oxford University Press, 2005.

[29] Department of Defense, "Summary of the 2018 National Defense Strategy of The United States of America; Sharpening the American Military's Competitive Edge," https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[30] Some analysts interpret this as cyberspace, while others contend that the emphasis throughout Russian doctrine is on information itself.

[31] The document is available at http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666. See also Statement of Timothy Thomas before the House Armed Services Subcommittee on Emerging Threats and Capabilities, March 15, 2017, at http://docs.house.gov/meetings/AS/AS26/20170315/105689/HHRG-115-AS26-Wstate-ThomasT-20170315.pdf.

election.[32] The report states that the Central Intelligence Agency, the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) have "high confidence" that Russian President Vladimir Putin "ordered an influence campaign in 2016 aimed at the US presidential election" in order to "undermine public faith in the US democratic process, denigrate Clinton, and harm her electability and potential presidency."[33] While much of the reporting refers to the cyber element of Russian activities, the series of network intrusions, reconnaissance, and data releases appear to be tactical weapons used in support of a broader information warfare campaign around the U.S. presidential election.

Data exfiltration from the networks belonging to both political parties could offer the Russian government insight into the negotiating strategies, redlines, foreign policy goals, and platforms of an incoming administration, whatever the election outcome. Cyber tools were also used to create psychological effects in the American population. The likely collateral effects of these activities include compromising the fidelity of information, sowing discord and doubt in the American public about the validity of intelligence community reports, and prompting questions about the legitimacy of the democratic process itself.

In February 2018, Special Counsel Robert Mueller indicted 13 Russian nationals for their involvement in the U.S. election.[34] These individuals were said to have worked for the Internet Research Agency (IRA), a Russia-based organization that focused most of its efforts toward the United States. The indictment alleges that the IRA sought to conduct what it called "information warfare" on the U.S. population through "fictitious U.S. personas on social media platforms and other Internet-based media." The indictment alleges that U.S. citizens unknowingly counseled these Russian operatives as to how to focus their activities.

The operatives also reportedly used social media to widen social divides, exploiting existing fractures in American society. Over 3,000 Russian-bought Facebook ads heightened tensions and fomented discord among racial, religious, and political groups, by targeting messages to users based on their demographics and political preferences.[35]

Some analysts contend that given the success of past efforts and the absence of retaliatory action, Russia will continue to pursue its election-related information warfare.[36] As Director of National Intelligence Dan Coats said in February, 2018, "there should be no doubt" that Russia sees the 2018 U.S. midterm congressional elections as a target. "We expect Russia to continue using propaganda, social media, false-flag personas, sympathetic spokesmen and other means to influence, to try to build on its wide range of operations and exacerbate social and political fissures in the United States."

[32] Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," January 6, 2017.

[33] For more information, see CRS Insight IN10635, *Russia and the U.S. Presidential Election*, by Catherine A. Theohary and Cory Welt.

[34] Text of the indictment is available at https://www.politico.com/story/2018/02/16/text-full-mueller-indictment-on-russian-election-case-415670.

[35] These ads were presented to the House Intelligence Committee in November 2017. See Shane, Scott, "These are the ads Russia bought on Facebook in 2016," *New York Times*, November 1, 2017.

[36] Greenberg, Andy, "Trump's Win Signals Open Season for Russia's Political Hackers," *Wired*, November 9, 2016. In a February 27, 2018, hearing before the Senate Committee on Armed Services, Admiral Rogers, Commander of U.S. Cyber Command and Director of the National Security Agency, suggested that Russian leaders see few consequences for their efforts to undermine U.S. institutions.

The nature of these activities, particularly tampering with a sovereign nation's internal democratic processes and systems, has raised questions as to whether they constitute an act of war or espionage. While some Russian doctrine suggests that these subversive activities are a way to "prepare the battlefield" in advance of a conflict, it may also be the conflict itself: information warfare is a way to weaken a militarily superior adversary without firing a single bullet.

Other activities conducted outside of cyberspace include production of pro-Russia television shows and broadcasts in Russian speaking areas of NATO, deploying soldiers in Ukraine for propaganda purposes, and the use of "little green men," armed soldiers without insignia, allowing plausible deniability of a military incursion in Crimea while creating fear and intimidation among the local population.[37]

China

The Chinese strategy of information warfare focuses on the use of what China calls "strategems" to build and maintain information superiority. These strategems help China compensate for its deficiencies in technology-based weapons, and may contain efforts to create cognitive errors and to influence the contents, process, and direction of thinking of an adversary. Cyberspace operations are used to achieve information dominance through reconnaissance and espionage, conducting network intrusions to steal and possibly alter data.

The Chinese concept of "Unrestricted Warfare" combines elements of information operations, cyberspace operations, irregular warfare, lawfare,[38] and foreign relations, carried out in peacetime, as well as in conflict. The United States is viewed as a militarily superior foe whose advantages can be overcome through strategy and information operations. The U.S. reliance on technology, both in the military and in the civilian population, creates a vulnerability that can be exploited, along with "theoretical blind spots" and "thought errors," such as the absence of a comprehensive theory in DOD doctrine that combines all elements of information warfare.[39]

In cyberspace, computer network espionage plays a large role in Chinese efforts to pursue a competitive advantage. In 2009, China was suspected of stealing large terabytes of design data for the F-35 Joint Strike Fighter from defense contractor Lockheed Martin's computers. In 2012, a Chinese version, the J-31, appeared to rival the F-35.[40] In 2014, a Chinese national was indicted for theft of sensitive trade secrets defense contractors, particularly data relating to Boeing's C-17 military transport aircraft.[41] Industrial espionage such as this yields economic benefits, as well as military and national security advantages for China, while eroding the technical superiority of the United States. Another concern with this type of espionage is that detailed knowledge of the F-35 and C-17 platforms could afford China the ability to hack a plane's command and control system,

[37] Shevchenko, Vitaly, "Little Green Men or Russian Invaders?", *BBC News*, March 11, 2014 http://www.bbc.com/news/world-europe-26532154.

[38] Popularized by General Charles Dunlap, the concept of lawfare is a form of asymmetric warfare consisting of the use of the legal system against a foe, by damaging or delegitimizing them, or winning a public relations victory. See Dunlap, Charles J., "Lawfare Today ... and Tomorrow," in *International Law and the Changing Character of War, 2011*; and Kettrie, Orde F., "Lawfare: Law as a Weapon of War," Oxford University Press, 2016.

[39] Wang Xiangsui and Liang Giao, "*Unrestricted Warfare" China's Master Plan to Destroy America*," Shadow Lawn Press, 2017.

[40] Weisberger, Marcus, "Did the Chinese theft of data on the US fighter jet and other weapons shrink the Pentagon's technical superiority?", *Defense One*, September 23, 2015.

[41] Department of Justice, Office of Public Affairs, "Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contrators' Systems to Steal Sensitive Military Information," March 23, 2016.

to alter its course or possibly disable it in a time of crisis. In addition, a network intrusion could allow an undetectable cyber weapon to be planted, lying dormant until activated during a conflict.

On the defensive side, China employs a combination of legal policies and information technology for censorship and surveillance of dissenters in a program called "The Golden Shield."[42] This is often referred to as "The Great Firewall" of China. In addition, the People's Republic of China actively promotes the idea of "cyber sovereignty," putting borders on the internet based on territorial integrity.[43] This may be a way for the government to bypass the democratic free-flow of information that the internet represents.

Reportedly, the CIA has chronicled China's information warfare activities inside the United States, where financial incentives such as personnel and support in funding are aimed at academic institutions and think tanks to dissuade them from research that paints China in a negative light.[44] In a February 2018 hearing before the Senate Intelligence Committee, FBI Director Christopher Wray described so-called Confucius Institutes, Chinese language and cultural centers at universities that may be used as espionage tools to influence public opinion or to stifle academic freedom by limiting or disallowing discussions on certain topics. China has invested heavily in the motion picture industry as a way to gain cultural and economic influence, though reportedly China's relationship with Hollywood has started to cool.[45]

China has also been propagating an image of itself as a peaceful, nonthreatening nation focused on internal development rather than the pursuit of international power. UN Statements such as President Xi Jinping's that China "will never pursue hegemony, expansion, or sphere of influence" exemplify these attempts at influencing perception. Chinese information warfare doctrine suggests that these tactics are part of a broader strategy of encouraging complacency in potential adversaries. Other tactics include using international fora to promote the idea of arms control for "information weapons" in order to maintain control over its own information apparatus and to level the playing field with technologically advanced powers.[46]

Islamic State

The Islamic State (IS) has pursued an IW strategy of accessing U.S. government computer systems for a variety of purposes. IS pursues five primary categories of activity when targeting United States computer systems: defacement, distributed denial of service, data theft, disabling websites, and data breaches.[47]

[42] Denyer, Simon, "China's Scary Lesson To the World: Internet Censorship Works," *Washington Post*, May 23, 2016, https://www.washingtonpost.com/world/asia_pacific/chinas-scary-lesson-to-the-world-censoring-the-internet-works/2016/05/23/413afe78-fff3-11e5-8bb1-f124a43f84dc_story.html?utm_term=.49ae25e59cbb

[43] "China Internet: Xi Jinping calls for 'Cyber sovereignty,'" December 16, 2015, http://www.bbc.com/news/world-asia-china-35109453.

[44] Johnson, Natalie, "CIA Warns of Extensive Chinese Operation to Infiltrate American Institutions," *Washington Free Beacon*, March 7, 2018.

[45] Faughdner, Ryan and Koren, James Rufus, "As China cools on Hollywood, the movie business looks closer to home for money," *Los Angeles Times*, November 12, 2017.

[46] Beginning in 1998, both Russia and China have backed proposals in the UN General Assembly's First Committee (Disarmament and International Security Committee) to establish an arms control agreement for cyberspace. See "Developments in the Field of Information and Telecommunications in the Context of Security," A/RES/53/70, as introduced by the Russian Federation, http://undocs.org/A/RES/53/70.

[47] CRS Report R41674, *Terrorist Use of the Internet: Information Operations in Cyberspace*, by Catherine A. Theohary and John W. Rollins.

The "Cyber Caliphate," a group of pro-Islamic State hackers also known as the "Islamic Cyber Army" (ICA) or "Islamic State Hacking Division," has a history of conducting a variety of operations within the information environment.[48] The Department of Homeland Security and the FBI issued a joint statement in December 2014 warning members of the U.S. military that the Islamic State of Iraq and Syria (ISIS) may be mining social media to create "kill lists" of human targets or identify potential sympathizers for recruitment.[49]

In 2015, the U.S. Central Command's social media sites such as Twitter and Facebook were taken over for a short period of time by hackers claiming to be affiliated with the Islamic State. While this hack may have caused no damage to Central Command's operations, it was apparently designed to create a perception of vulnerability and weak U.S. national security capabilities. In April 2017, a pro-ISIS group claims to have hacked the State Department's website, stolen data, and released a kill list of U.S. government officials.[50] In addition, defacing government websites and redirecting web traffic are tactics used by the Islamic State to project its power online.

For the past several years, propaganda units of IS have been actively spreading their message through social media platforms such as Twitter, Facebook, and YouTube, as well as through radio broadcasts and news services. Videos showing the beheadings of Western hostages and the immolation of a caged Jordanian fighter pilot have made international headlines. Most recently, IS released a propaganda video showing an attack on U.S. soldiers in Niger that killed four Americans. Parts of this video were aired on television news shows.[51] Videos such as these appear intended to convey the perception of IS as winning against a weakened and vulnerable U.S. military. Islamic State's media arm itself is intended to appear to be a formalized, bureaucratic organization, thereby legitimizing IS and giving the appearance of an actual state. In 2015, then-FBI Director James B. Comey described these propaganda units as legitimate military targets.[52]

North Korea

Since its founding in 1949, North Korea has conducted an array of IW activities designed to promote its interests. These have been particularly active in South Korea and Japan, where North Korea has cultivated sympathetic followers. Its actions were particularly influential during South Korea's period of military dictatorship, which ended in 1988, but they have continued since then in an attempt to influence South Korean politics as well as the North Korea policies of outside powers, including the United States. More recently, North Korea has been complementing these traditional information warfare activities with an increasingly capable cyber program.

In 2014, the run-up to the scheduled Christmas Day release of *The Interview*, a film depicting the assassination of North Korean leader Kim Jong Un, North Korea's Foreign Ministry called the film "the most blatant act of terrorism and war" and threatened a "merciless countermeasure."[53] On November 24, 2014, Sony experienced a cyberattack that disabled its information technology

[48] Fahmi, Mohammed, "Cyber-Jihad is Becoming A Priority for the Islamic State," European Strategic Intelligence and Security Center, October 26, 2015.

[49] Ross, Brian and Meek, James, "ISI Threat at Home: FBI Warns US Military about Social Media Vulnerabilities," at abcnews.go.com/international/isis-threat-home-fbi-warns-us-military-social/story?id=27270662.

[50] Bennett, Cory, "Pro-ISIS hacking group leaks 'kill list' of US government officials," *The Hill*, April 26, 2016.

[51] Martin, David, "ISIS propaganda video shows U.S. soldiers under attack in Niger," *CBS News*, March 4, 2018.

[52] Miller, Greg and Mekhennet, Souad, "Inside the surreal world of the Islamic State's propaganda machine," *Washington Post*, November 20, 2015.

[53] For more information, see CRS Report R44912, *North Korean Cyber Capabilities: In Brief*, by Emma Chanlett-Avery et al.

systems, destroyed data, damaged computer workstations, and released internal emails. North Korea denied involvement in the attack but praised hackers, called the "Guardians of Peace," for having done a "righteous deed."[54] Emails followed, threatening "9/11-style" terrorist attacks on theaters scheduled to show the film, leading some theaters to cancel screenings and for Sony to cancel its widespread release, although U.S. officials claimed to have "no specific, credible intelligence of such a plot."[55] The FBI attributed the attacks to the North Korean government.[56]

Independent of the level of economic and physical damage that Sony suffered as a result of these cyberattacks, one could argue that the incident represents a successful use of IW to achieve political ends. Some questioned whether North Korea had developed a sophisticated cyberattack force, using these attacks to demonstrate its increasing ability to pursue political goals and thereby raise its profile on the international stage. Others pointed to the common use of proxies or mercenary hackers to conduct relatively simple cyber operations as a form of political protest or "cyber riot." Whether or not the North Korean government conducted the attacks or outsourced to a proxy organization, the cyberattacks, in concert with threats of physical destruction, affected the decisionmaking process of a private company, exploited the human element of fear in a civilian population, imposed extra-territorial censorship, and triggered a response from the U.S. government.[57]

North Korea appears to be engaging in increasingly hostile cyber activities, including theft, website vandalism, and denial of service attacks. Some cybersecurity analysts, however, question whether the country has developed the technical capability to conduct large-scale destructive attacks on critical infrastructure. Some observers suggest that, because there is little visibility into North Korea's activities, the possible threats from North Korean cyber activities are often inflated. An assessment released by the Korea Economic Institute found that the international community's "fears of the unknown increase the risk of threat inflation dramatically."[58] These analysts contend that while North Korea may have the capability to undertake global cyber nuisance or theft-motivated activities, the nation lacks the ability to undertake operations that are "complex or as devastating as the Stuxnet attack, a computer virus that disrupted Iran's nuclear program."[59] The ambiguous threat of North Korean cyberattack ability, or fear of the unknown, creates a psychological effect that could perhaps deter some countries from conducting cyberspace operations on North Korean networks.

Outside of cyberspace, North Korean use of the information environment include its presence at the 2018 Winter Olympics, propaganda photos, videos, and claims in the media that place North Korea and its leadership in a favorable light, contrasting it with other countries such as South Korea and the United States. Some argue that U.S. journalists' coverage of North Korea and the Olympics suggest that the event was a propaganda win for North Korean leaders.[60] Likewise, recent propaganda posters and stamps for the 70th anniversary of the founding of North Korea

[54] "North Korea: Sony Hack a Righteous Deed But We Didn't Do It," *The Guardian*, December 7, 2014.

[55] FBI National Press Office, "Update on Sony Investigation," December 19, 2014, https://www.fbi/gov/news/pressrel/press-releases/update-on-sony-investigation.

[56] Ibid.

[57] Grossman, Andrew, "U.S. Weights Options to Respond to Sony Hack, Homeland Security Chief Says," *Wall Street Journal*, December 18, 2014.

[58] Dr. Alexandre Mansourov, "North Korea's Cyber Warfare and Challenges for the U.S.-ROK Alliance, Korea Economic Institute of America, Academic Paper Series, December 2, 2014.

[59] Edwards, Will, "North Korea as a Cyber Threat," *The Cipher Brief*, July 1, 2016.

[60] Tani, Maxwell, "American Media Just Can't Resist North Korean Propaganda," *The Daily Beast*, February 2, 2018, at https://www.thedailybeast.com/american-media-just-cant-resist-north-korean-propaganda.

declare "Victory in all fronts."[61] The North Korean government has also tried to use information campaigns to set the agendas of international negotiations such as inter-Korean dialogue and nuclear talks with the United States.

Iran

Similar to China, Iranian information operations target and discredit dissenters and adversaries, both domestic and foreign—to include journalists, online media activists, and human rights defenders—and limiting or prohibiting attempts by protesters to coordinate and organize.[62] The Islamic Republic of Iran Broadcasting (IRIB) corporation runs the government's foreign media arms, which are largely considered propaganda tools as opposed to public diplomacy.[63] In cyberspace, the Iranian government shut down social media platforms and disrupted internet access during nationwide protests in January 2018.[64] Iran may also be seeking a capability to disable or destroy critical infrastructure through cyber means.

Beginning in 2011, a wave of cyberattacks on U.S. financial institutions disrupted banking operation and denied some customers from online access to their accounts. Roughly four dozen banks, including JPMorgan Chase, Bank of America, Capital One and PNC Bank, were besieged by crippling denial of service attacks that lasted for over a year. Some have speculated that these were conducted in retaliation for the Stuxnet worm, which disabled the computer systems that controlled nuclear centrifuges at Iran's main nuclear enrichment plant in 2010.[65]

A cyber intrusion into the computer program controlling the sluice gate to the Bowman Dam in Rye, NY, appeared be an effort to take over the computer controls to the dam itself. Any attempt to do so failed, however, because the dam was under repair and offline.[66]

According to an indictment by the U.S. Department of Justice, the perpetrators for both the bank and dam incidents are associated with Iran's Islamic Revolutionary Guards Corps, a unit of which is the Iranian Cyber Army (ICA), which runs military cyber operations.[67] Iran openly encourages hacker groups to conduct offensive cyberspace operations. Hackers deface websites, steal and leak content, and may be involved in cyber espionage operations.[68] The Iranian Cyber Army (ICA) has been implicated in several website attacks, including one against Twitter in 2009 that proclaimed support for Iran's Supreme Leader Ali Khamenei. Other attack targets were the Voice

[61] Telegraph News, "'Victory in all fronts'—North Korea releases new propaganda posters and stamps for 70th anniversary," February 2, 2018, at https://www.telegraph.co.uk/news/2018/02/02/north-korea-releases-new-propaganda-posters-70th-anniversary/

[62] Center for Human Rights in Iran report, "Guards at the Gate: The Expanding State Control Over the Internet in Iran," January 2018.

[63] Tiedeman, Anna, "Islamic Republic of Iran Broadcasting: Public Diplomacy or Propaganda?", *al Nakhlah*, Spring 2005. http://www.fletcher.tufts.edu/`/media/Fletcher/Microsites/al%20Nakhlah/archives/pdg.tiedman.pdf.

[64] Maza, Cristina, "Iran Protests: Government Took Control of the Internet to Silence Dissent, Report Says," *Newsweek*, January 10, 2018.

[65] Capaccio, Tony, "US General: Iranian Cyberattacks are Retaliation for the Stuxnet Virus," *Business Insider*, January 18, 2013.

[66] Berger, Joseph, "A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case," *New York Times*, March 25, 2016.

[67] Department of Justice, Office of Public Affairs, "Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector," March 24, 2016.

[68] Department of Defense, "Fiscal Year 2016 Report on the Military Power of Iran," January 2017.

of America in 2011 after the United States rhetorically supported Iran's opposition Green movement, and regime opposition websites in 2013 just before the presidential election.

Acts of War and Other Questions for Congress

Some policymakers have questioned whether tampering with, interfering with, or otherwise influencing a sovereign nation's democratic processes in an IW campaign is an act of war that could trigger a military response. A similar question is whether a cyberattack that falls below the threshold of damage and destruction resulting from a kinetic event could be considered an armed attack or use of force under international law, or whether data breaches of military networks or theft of sensitive defense information constitute an act of aggression rather than espionage.

Other questions Congress may consider include whether the United States has a strategy in place to match the robust IW strategies of its competitors, and whether the U.S. government has institutions, organization, and programs to wage and win an information war or to deter foreign information operations.

With respect to cyberspace and information operations, the structures supporting each set of capabilities are currently bifurcated within the Department of Defense. In addition, cyberspace operations tend to focus on computer network attacks rather than the cognitive and strategic effects of information. As such, Congress may explore whether current organizational and doctrinal constructs support the full integration of these capabilities to maximize their effects, and whether ongoing conceptual confusion has inhibited DOD's ability to respond to IW challenges.

When responding to foreign IW activities on the United States, Congress may consider whether authorities are in place for DOD to conduct counter-IO, and if other interagency entities are authorized and resourced to conduct coordinated efforts. Another consideration may be the efficacy of IW as a military function or a whole-of-government responsibility.

Author Contact Information

Catherine A. Theohary
Specialist in National Security Policy, Cyber and
Information Operations
ctheohary@crs.loc.gov, 7-0844