CRS INSIGHT

Information Warfare: Russian Activities

September 2, 2016 (IN10563)

|

Related Authors

- Catherine A. Theohary
- Kathleen J. McInnis

|

Catherine A. Theohary, Specialist in National Security Policy and Information Operations (ctheohary@crs.loc.gov, 7-0844)
Kathleen J. McInnis, Analyst in International Security (kmcinnis@crs.loc.gov, 7-1416)

Pointing to several recent high-profile events, media reports suggest that Russia is engaging in activities that some may describe as Information Warfare (IW): the range of military and government operations to protect and exploit the information environment. These alleged events include "hacks" of servers of U.S. political parties and other groups; releases and possible manipulation of sensitive documents in an attempt to influence the upcoming U.S. presidential election; and the manipulation of publicly available information on Russian activities in Ukraine. The scale and frequency of attacks on U.S. information architecture raise issues for the United States, including whether the Department of Defense adequately conceptualizes and is organized to counter IW.

Russian Conceptualization of IW

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.
- To shape a favorable international response to the deployment of its military forces, or military forces with which Moscow is allied.

Tactics used to accomplish these goals include damaging information systems and critical infrastructure; subverting political, economic, and social systems; instigating "massive psychological manipulation of the population to destabilize the society and state"; and coercing targets to make decisions counter to their interests. Recent events suggest that Russia may be employing a mix of propaganda, misinformation, and deliberately misleading or corrupted disinformation in order to do so. And while Russian organizations appear to be using cyberspace as a primary medium through which these goals are achieved, the government also appears to potentially be using the physical realm to conduct more traditional influence operations including denying the deployment of troops in conflict areas and the use of online "troll armies" to propagate pro-Russian rhetoric.

Examples of Possible Russian IW

Collection and analysis of information is routinely conducted by intelligence agencies of other countries. Yet to many scholars and practitioners, recent events appear to have transitioned from routine activities to more aggressive operations. These events include:

- **The theft and release of sensitive Democratic National Committee (DNC)** emails just prior to the DNC convention in July, likely intended to disrupt the convention's proceedings. Although a "hacktivist" known as Guccifer 2.0 claimed sole responsibility for stealing and releasing the emails through Wikileaks, experts both in and out of the U.S. government reject that claim, citing digital forensic evidence to the contrary.
- **Some experts assert that Wikileaks itself** is a proxy for Kremlin intelligence agencies, used as a vehicle to spread a combination of accurate and manipulated information as part of an overall disinformation campaign. Others contend that Wikileaks states its mission is to improve transparency. Still, it tends to focus its efforts on U.S. or NATO allied governments rather than Russia.
- **Concerns that Russia may tamper with the U.S. election in November**. The FBI released an "unprecedented" notification on August 18, 2016, stating that breaches were found in several state-level voter databases. As the purpose is unclear, Senate Minority Leader Harry Reid asked the FBI to investigate the possibility of Russian interference in the election. On August 30, 2016, FBI Director James Comey stated that "We take very seriously any effort by any actor, including nation-states, and maybe especially nation-states, that moves beyond the collection of information about our country and that offers the prospect of an effort to influence the conduct of affairs in our country."
- **Concerns that the Panama papers leak was orchestrated at President Vladimir Putin's behest**. The papers embarrassed Western political figures by exposing corrupt financial practices, and while Putin and his affiliates were also implicated, there was no direct evidence linking him to any such corruption.
- **Covert Russian involvement in Ukraine** including the deployment of troops for propaganda effects.

DOD Conceptualization of IW

The Department of Defense conceptualization of IW has evolved along with changing definitions for related concepts and capabilities. IW currently has no formal definition in DOD doctrine, but is commonly understood as the process of protecting one's own sources of battlefield information while seeking to deny, degrade, corrupt, or destroy those of an adversary. The means through which this may be accomplished are known as Information Operations (IO). IO takes place within the information environment, which consists of individuals, organizations, and systems that collect, process, disseminate, or act on information. Related dimensions include the physical, including command and control systems; informational, where information is stored, disseminated, and protected; and cognitive, which encompasses the minds of those who use information. An information-related capability is a tool, technique, or activity that can be used within the information environment to create effects and operationally desirable conditions.

Following the evolution in conceptualization and definitions, organizational constructs and components related to IO have also been restructured. Until recently, IO was divided into five subsets: computer network operations, psychological operations, electronic warfare, military deception, and operation security. With the growing prevalence of large-scale, seemingly state-sponsored cyber attacks and with the creation of the U.S. Cyber Command, cyberspace operations, including offensive and defensive, were separated from information operations doctrine. IO is now defined 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 decisionmaking of adversaries and potential adversaries while protecting our own.

Cyberspace, as a global domain within the information environment, is considered to be a battlefield through which some information-related capabilities may be deployed. While joint publications note the relationship between cyberspace operations and information operations, the structures supporting each set of capabilities are bifurcated. Additionally, 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. Another consideration may be the efficacy of IW as a military

function or a whole-of-government responsibility.