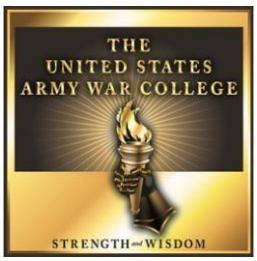
Strategy Research Project

Tinker, Terrorist, Cyberpunk, Spy: Public Disclosure Websites and Extremist Threats

by

Mr. Nathan Timothy Ray
Interagency



United States Army War College
Class of 2015

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2015	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Tinker, Terrorist, Cyberpunk, Spy: Public Disclosure Websites and Extremist Threats

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Mr. Nathan Timothy Ray
Interagency

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Dr. Paul Rexton Kan
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,260

14. ABSTRACT

Public disclosure websites (PDW)—sites like WikiLeaks—constitute a serious security challenge to the United States and other nations. PDW activists are dedicated to exposing sensitive government and commercial information in the belief that they are acting in the public good. As a result, PDWs have revealed hard-to-find, strategic and tactical level information that benefits the resiliency and operations of insurgent, terrorist, and criminal groups. To date, there is no evidence linking PDWs to an attack by violent nonstate groups, but this threat is almost certain to grow as Internet access expands globally. Given the high likelihood of future leaks, the U.S. Government should adopt stronger controls to safeguard information, including new legislation to address leaking, as well as tailoring “need to share” practices. Left unchallenged, PDWs imperil the ability of the United States to counter violent nonstate groups.

15. SUBJECT TERMS
Internet, Intelligence, Counterintelligence, Insurgency, Organized Crime

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	34	

USAWC STRATEGY RESEARCH PROJECT

Tinker, Terrorist, Cyberpunk, Spy: Public Disclosure Websites and Extremist Threats

by

Mr. Nathan Timothy Ray
Interagency

Dr. Paul Rexton Kan
Department of National Security and Strategy
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Tinker, Terrorist, Cyberpunk, Spy: Public Disclosure Websites and Extremist Threats
Report Date:	01 April 2015
Page Count:	34
Word Count:	5,260
Key Terms:	Internet, Intelligence, Counterintelligence, Insurgency, Organized Crime
Classification:	Unclassified

Public disclosure websites (PDW)—sites like WikiLeaks—constitute a serious security challenge to the United States and other nations. PDW activists are dedicated to exposing sensitive government and commercial information in the belief that they are acting in the public good. As a result, PDWs have revealed hard-to-find, strategic and tactical level information that benefits the resiliency and operations of insurgent, terrorist, and criminal groups. To date, there is no evidence linking PDWs to an attack by violent nonstate groups, but this threat is almost certain to grow as Internet access expands globally. Given the high likelihood of future leaks, the U.S. Government should adopt stronger controls to safeguard information, including new legislation to address leaking, as well as tailoring “need to share” practices. Left unchallenged, PDWs imperil the ability of the United States to counter violent nonstate groups.

Tinker, Terrorist, Cyberpunk, Spy: Public Disclosure Websites and Extremist Threats

> As he [Mohammed] called me by name to stand, he said, "Go get me information about those people and do not alarm them about me."
>
> —*Military Studies in the Jihad Against the Tyrants: The Al-Qaeda Training Manual*

In April 2011, a group of Libyan fighters hunkered behind a screen of trees near their hometown of Yefren, in the Nafusa Mountains southwest of Tripoli. They were frightened and unsure of their next move. Nearby, government forces were bombarding the town with rockets tipped with high-explosives. If they attacked, did the rockets pose a threat? They needed intelligence. The leader's cell phone rang. It was a response to his request for information. Via Skype, two Libyan nationals, one in Finland, the other in the United Kingdom, briefed the leader—the British contact had trained on the same rocket launchers during his compulsory military service under the Qaddafi regime. Because the fighters were so close, he told the leader, the rockets would overshoot them if they attacked. The British contact also indicated that Qaddafi's soldiers probably were some distance away, remotely firing the rockets using an electric cable. Armed with this intelligence, the Libyan fighters successfully assaulted the batteries.[1]

The Public Disclosure Website Phenomenon

This vignette from the recent fighting in Libya illustrates that the Internet and related technologies[2] are improving the intelligence gathering capabilities of violent nonstate actors—insurgents, terrorists, and crime groups. It also highlights that the *quality* of Internet-based intelligence information is improving. Now, fighters can mine the proliferation of government, news, and military-interest websites for information that potentially provides immediate tactical advantages, as well as enhances a group's

resiliency against adversarial intelligence and security efforts. This latter kind of information, although not "readily actionable," might be more valuable to an armed group over time because it benefits a group's "learn/grow process," influencing and informing how fighters analyze adversarial threats, including strategic-level challenges.[3] Properly employed, the Internet may therefore serve nonstate groups as an adjunct case officer, counterintelligence officer, and intelligence analyst.

From this perspective, the advent of *public disclosure websites* (PDW)—sites like WikiLeaks (wikileaks.org) or the Federation of American Scientists' Secrecy Project (fas.org)—is particularly worrisome. PDWs are dedicated to the belief that "citizens deserve more access to information that the powers that be hold in secret" and encourage exposure of sensitive government and commercial information out of conviction that they are serving the public good.[4] As a result, PDW disclosures have harmed "governments and corporations in ways that have much more wide-ranging implications than many other global social movements before them, from economic to security threats."[5] PDW activists may not espouse violence or crime, and most do not, but their efforts to date have revealed hard-to-find information, including strategic-level information and analysis, that benefits insurgents, terrorists, and criminals.

The PDW phenomenon adds a new element to discussions since the 9/11 attacks about the use of the Internet by violent nonstate actors. Much of the focus has concentrated on their ability to use the Internet for propaganda, fundraising, communications, or computer network attacks.[6] Some commentators, however, note that the Internet is a neutral operational environment for nonstate actors, who are vulnerable to online surveillance by authorities, as well as their own paranoia regarding

this surveillance.[7] A few even argue that “the Internet is not a force multiplier for terrorist organizations.”[8] Too often, these discussions do not explore, or overlook altogether, Internet-based intelligence collection by armed groups, an ironic oversight given widespread acknowledgement that greater understanding of nonstate actor intelligence practices is crucial to countering extremists.[9]

Nonstate groups recognize the value of open-source information available through PDWs and the Internet. For example, the website for the Muslim Hackers Club, noted for developing cyber attack tools, linked to PDWs purporting to disclose U.S. Secret Service code names and radio frequencies.[10] Al-Qa’ida has long-recognized the importance of publicly-available information, which the Internet has made easier—and safer—to find. “Using [openly available information] and without resorting to illegal means,” one operations manual instructs, “it is possible to gather at least 80% of information about the enemy…The one gathering information with this public method is not exposed to any danger whatsoever.”[11] Another manual advises fighters to employ a “computer specialist” for intelligence collection, who can “enter and download information as required, whether this be images, video, secret documents, statements, or textual reports.”[12]

By surveying the PDW phenomenon—introducing a new term and nomenclature to describe these sites—and the intelligence gathering practices and needs of nonstate groups, this paper demonstrates that PDWs are of significant intelligence value to insurgents, terrorists, and crime groups. PDWs potentially have and will continue to supply extremists with critical pieces of intelligence that benefit their operations and long-term survival. As a result, the efforts of PDW activists constitute a serious security

challenge to the United States and other nations. Therefore, the U.S. Government should continue strengthening its information assurance controls, to include re-evaluating “need-to-share” mindsets sanctioned in the wake of the 9/11 attacks, because PDWs rely on anonymous leakers and self-described whistleblowers like Edward Snowden for site content.

The Lunev Axiom Re-Validated

PDWs are enlarging the pool of valuable operational information and analysis for extremists. A few commentators downplay the potential strategic effect of PDW-related leaks arguing that the total amount of classified government information, which continues to grow, vastly outweighs the number of sensitive documents currently available online.[13] In other words, “the count of leaked [documents] tells us nothing about the significance of a breach.”[14] While accurate, such a critique overlooks the potential *sensitivity* of the exposed information. Even a single improperly disclosed document can wield tremendous damage to national security, depending on its content. For example, WikiLeaks published documents that indicated Washington was interested in Abbottabad days before the U.S. operation against Osama bin Ladin, almost compromising the raid.[15] Similarly, the U.S. Department of Defense warned in March 2010 that “some 2,000 pages of documents WikiLeaks released on equipment used by coalition forces in Iraq and Afghanistan…could be used by foreign intelligence services, terrorist groups and others to identify vulnerabilities, plan attacks and build new [improvised explosive] devices.”[16]

Moreover, PDWs already may be helping to strengthen the long-term resiliency of nonstate groups against military, law enforcement, and intelligence operations. Even before Snowden’s revelations, “Jihadist technology …[was] so sophisticated and

secretive" that the National Security Agency (NSA) was unable to monitor their communications, despite using collection methods "specifically designed to uncover terrorist plots."[17] Now, groups like the Islamic State in Iraq and Syria (ISIS) boast about using "Snowden approved" encryption to protect their communications,[18] which suggests that at least some fighters have further upgraded security measures due to Snowden's leaks. Indirectly, nonstate groups also will be using more secure off-the-shelf electronic devices and digital technologies in the future, as manufacturers and service providers like Apple, Google, Yahoo, and Facebook have scrambled to protect user information in response to the public outcry over Snowden's revelations.[19]

These developments highlight the continuing validity of the Lunev Axiom of intelligence, first coined by veteran U.S. intelligence officer James Bruce to describe the negative impact of Cold War-era press leaks on U.S intelligence and military operations and capabilities. The Lunev Axiom states that "classified information disclosed in the press is the effective equivalent of intelligence gathered through foreign espionage."[20] Bruce based his observation on a comment from former Soviet military intelligence officer Stanislav Lunev, who defected to the United States in 1992. "I was amazed—and Moscow was very appreciative—at how many times I found very sensitive information in American newspapers," Lunev later recalled. "In my view, Americans tend to care more about scooping their competition than about national security, which made my job easier."[21]

According to Bruce, press leaks that reveal intelligence techniques and operations give adversaries the opportunity to develop denial and deception countermeasures, resulting in a decline in the effectiveness of intelligence collection

efforts—and raising the potential that intelligence collection can be defeated.[22] Bruce notes that this problem is more acute today, because leaked materials are now easily disseminated and researched electronically, allowing rapid compilation and comprehensive review.[23] Former NSA and Central Intelligence Agency (CIA) director Michael Hayden echoed this concern in the wake of the WikiLeaks revelations in 2010:

> If I had gotten this trove on the Taliban or Al-Qaeda, I would have called this priceless. If I'm head of Russian intelligence, I'm getting my best English speakers and saying, “Read every document, I want you to tell me how good are these guys? What are their approaches, their strengths, their weaknesses and blind spots?”[24]

Nonstate actors almost certainly view sensitive materials published by PDWs as a similar windfall of valuable intelligence.

Intelligence Agencies of the People

PDWs are dedicated to exposing sensitive government and commercial information in the belief that ordinary citizens deserve greater access to information held in secret by “the powers that be.”[25] The most extreme PDW activists believe that “Information does not just want to be free; it longs to be free. Information expands to fill the available storage space.”[26] Virtually all PDWs actively encourage and abet leaking or self-described whistleblowing, as well as declassification of U.S. Government materials through the Freedom of Information Act (FOIA). Activists also actively promote the use of encryption and Internet anonymizing programs, such as The Onion Router or Tor, a program that enables secure Internet browsing, because these tools allow Internet users to “to create regions free from the coercive force of the outer state.”[27] More practically, these tools allow leakers and self-described whistleblowers to divulge sensitive information anonymously and communicate securely with activists.

In essence, PDWs are not new. They are rooted in the activist journalism of the Twentieth Century and Vietnam-era disclosures, such as *The Pentagon Papers* and Philip Agee's disclosures of CIA operations.[28] Yet, PDWs are distinguished from their antecedents in several ways. First, many PDWs and their supporters view themselves to be "the intelligence agency of the people,"[29] because they are at the forefront of Internet-based *sousveillance* efforts. Sousveillance, or inverse surveillance, is the "observation from below of more powerful organizations and people."[30] This concept can be traced to the videotaped beating of Rodney King in 1991, and is now often characterized as informal networks of citizens who record the activities of police and government authorities using cell phone cameras and post the footage online due to a desire to curb the perceived excesses of the state.[31] According to one observer, however, the WikiLeaks disclosures in 2010 were "the most controversial and publicized sousveillance" effort to date[32]—at least until Snowden's revelations.

Second, PDWs are technologically poised to enable and take advantage of leaks, as well as exploit the growing amount of information that governments and businesses are posting online. Such a posture increases the potential "scale and scope" of PDW-enabled disclosures over past incidents of leaking and ensures that improperly disclosed materials will proliferate rapidly over the Internet.[33] Most PDWs encourage whistleblowing and leaking by enabling secure "drop boxes" where individuals can anonymously and securely submit sensitive materials,[34] in addition to providing free software that protects Internet users from online surveillance. WikiLeaks, for example, pioneered the use of Skype, which scrambles transmissions, Pretty Good Privacy, a free encryption program, and the Tor browser, which anonymizes Internet usage by

routing activity through a network of approximately 2,000 volunteer computer servers worldwide.[35] Similarly, a rival site, GlobaLeaks (globaleaks.org), sponsors Tor-based software to create a peer-to-peer "leak amplification network."[36]

Third, PDWs are an artifact of the Web 2.0 philosophy and culture. As with other Web 2.0 entities, such as jihadist websites, PDW users and supporters participate in a virtual community, helping to produce and shape website content, instead of just passively consuming information.[37] This interactive characteristic fosters PDW relationships with other online activist entities, most notably the shadowy hacktivist collective Anonymous, which shares similar beliefs regarding free speech online and information freedom.[38] The Web 2.0 ethos also makes Snowden's recent leaks a part of the PDW phenomenon. Snowden justified his actions as sousveillance, improperly disclosed sensitive U.S. documents using the same encryption and anonymizing tools and techniques that PDWs promote, received legal support from WikiLeaks, at least initially, and ongoing publication of leaked information is occurring online.[39]

Finally, PDWs are creating a new "complex media ecology" through relationships with traditional media, according to observers.[40] In part, this has occurred because the sheer volume of leaked materials on sites like WikiLeaks limits the public's ability to interpret the information, defeating activist efforts to stoke the kind of indignation that leads to political reform.[41] For example, after seeing the muted public response to large releases of U.S. military and diplomatic documents in 2010, WikiLeaks turned to *The New York Times*, *The Guardian*, and *Der Spiegel* for assistance in deciphering the exposed content—U.S. military and diplomatic acronyms, classification information, and other arcana—and shaping it into more accessible stories, including the redaction of

names.[42] PDWs have forged relationships with traditional media outlets also to overcome limited funding, as most sites rely heavily on donations for operations, and diffuse the impact of potential litigation.[43]

For their part, traditional media outlets have embraced PDWs because they "dramatically increased the ease with which reporters, editors, and publishers can evade laws or regulations pertaining to the publication of classified information."[44] Such access to leaked information has multiple benefits for established media, not the least of which is increased circulation, a critical need given that online news consumption has dramatically depressed print media sales and widened the number of Internet venues delivering news and information. Stories about and incorporating leaked information also have revitalized the "campaigning reputations" many established media outlets forged in the Twentieth Century and burnished their status for "high-quality journalism," which PDWs lack. In short, traditional media outlets will continue to embrace PDWs to remind readers "they are still key players in the political game."[45]

Secret Archives on Your Desktop

PDWs are digital libraries, meaning that information stored on the site can be searched easily with key words and archived open-endedly. Site content is also available indefinitely on the Internet, whether through PDW mirror sites or programs like the "Wayback Machine" (archive.org), which digitally stores Internet content.[46] Indeed, many PDWs, such as WikiLeaks, use mirror sites to operate despite limited funds and government efforts to shut down or block access to them.[47] In other words, sensitive information published by a PDW is and will be available to any user for the foreseeable future, including extremists. Moreover, the site content of many PDWs continually

grows. As of 2011, for example, WikiLeaks received sensitive documents “about thirty times a day,” according to one observer.[48]

The digital nature of PDWs therefore benefits nonstate groups in several ways. PDWs are easily accessed and the Internet’s global spread now means any armed group will be able to retrieve and review leaked information as it becomes available on these sites. PDWs also help solve information storage and retrieval issues that have traditionally plagued nonstate groups seeking to preserve intelligence information. The pressure on many armed groups and the lack of safe havens means that fighters must compartmentalize functions like intelligence gathering and records-keeping to preserve these capabilities in case of compromise. Accordingly, valuable information can and does get misplaced or captured. As former Provisional Irish Republican Army (PIRA) operative Brendan Hughes remembered in 2004:

> In 1987, I came across a dump, a bundle of intelligence reports that had been lying there from 1974, and what had happened was the intelligence officer whose stuff it was was killed and no one knew where he had his stuff hidden. That happens in a guerilla organisation (sic)—a lot of the intelligence is lost like that because you do not have a central control where you can gather and hold intelligence. So, a lot of it is done by word of mouth…by memory. A lot of it has gone…it’s not a great system.[49]

PDWs, in addition to “cloud storage” options, help solve such conundrums for fighters.

The number of PDWs, however, may challenge the ability of extremists to monitor them. Virtually all PDW activists provide support to leakers and self-described whistleblowers, but they are not uniform in their views regarding unauthorized disclosures. These differences of opinion have led to the creation of multiple sites and shape how site owners release and analyze leaked materials and declassified documents. The following broadly sketches the PDW community.

Disruptive Sites

Disruptive sites are the most visible and notorious PDWs. Activists associated with them, such as Julian Assange, WikiLeaks' founder and chief spokesperson, are willing to expose all types of sensitive information, regardless of proprietary or intellectual property controls, in the belief they are serving the greater public good.[50] Disruptive PDWs include WikiLeaks, the most prominent PDW to date, and Cryptome (cryptome.org), a less-well known competitor that has been active since the 1990s and is probably the oldest PDW in operation.[51] The WikiLeaks revelations in 2010 and the resulting publicity spawned a range of lesser known and as yet less effectual copycat sites like BalkanLeaks (balkanleaks.eu), OpenLeaks (openleaks.org), founded by a former WikiLeaks member, and GlobaLeaks, which seeks to help "anyone…easily set up and maintain an anonymous whistleblowing platform."[52]

Disruptive PDWs have improperly disclosed a range of sensitive government materials, in addition to the tens of thousands of U.S. military and diplomatic documents revealed by WikiLeaks in 2010. For example, Cryptome has published "the names of 2,619 CIA sources, 276 British intelligence agents, 600 Japanese intelligence agents," as well as imagery of sensitive U.S. Government sites.[53] Some disruptive PDWs even apparently specialize in certain disclosures. Cryptocomb (cryptocomb.org), a new site, seems exclusively focused on unmasking alleged CIA officers and covert facilities.[54]

Government Transparency Sites

Numerous PDWs are dedicated to government transparency in the United States alone, many of which are less extreme than disruptive sites and take a more pragmatic approach to secrecy in government and the private sector.[55] For example, Stephen Aftergood, director of the Federation of American Scientists' Secrecy Project—

recognized as one of the “most important” government watchdog sites—seeks to “‘challenge unwarranted secrecy and to promote reform of national security information policy and practice,’” but “also believes that some information should be classified.”[56] Aftergood seeks to use the Secrecy Project to strike a “balance between what government should keep classified and what the American public should be able to see.”[57] Likewise, many government transparency activists, such as Daniel Ellsberg, who maintains his own personal website (ellsberg.net), have been engaged in watchdog efforts for decades and do not share the same zeal as Assange and his cohorts.

At the same time, the efforts of government transparency sites potentially benefit nonstate actors in several ways. A number are at the forefront of FOIA efforts to declassify government documents, providing both insight about the FOIA process and updates about newly declassified documents, whistleblowing, and leaked information—sometimes several times a week.[58] Some sites also serve as clearinghouses for whistleblowing and whistleblowers, including links to resources to enable the filing of complaints.[59] In addition, some government transparency sites link to or repost leaked information and provide, as does the Secrecy Project, insightful analysis regarding security and intelligence issues.

Media-Enabled Sites

As noted above, traditional media developed relationships with PDWs in the wake of the WikiLeaks revelations in 2010, but a handful of outlets, such as *The Wall Street Journal*, created their own leaker sites, apparently using the same anonymizing and encryption tools that PDWs employ.[60] This allows these outlets a freer hand in evaluating leaked information and directly shaping any subsequent story related to its release. However, until the Snowden revelations in 2013, only one of these sites, *Al*

Jazeera's "Transparency Unit," participated in a noteworthy and large-scale disclosure of sensitive materials. In January 2011, the Transparency Unit released approximately 1,700 files consisting of diplomatic correspondence, memos, e-mails, minutes of private meetings, strategy papers, and Powerpoint slides related to the Israeli-Palestinian peace process from 1999-2010.[61] The leak potentially had greater political impact than the WikiLeaks revelations, according to observers.[62]

Independent Sites and Blogs

An untold number of individuals with varying political agendas are routinely linking to, reposting, and blogging about sensitive and declassified information published to the Internet. Some individuals reach wide audiences, like security expert Bruce Schneier (schneier.com), who publishes the popular "Crypto-Gram" monthly e-mail newsletter.[63] Independent sites also may directly receive leaked information, such as occurred in the case of former Federal Bureau of Investigation (FBI) linguist Shamai Leibowitz, who was convicted in May 2010 of passing classified materials to a blogger.[64]

The Heartbeat of the War

Violent nonstate actors seeking to exploit information disclosed by PDWs almost certainly have created and will create new security challenges for the United States and other countries. Nonstate groups collect intelligence because "chance and uncertainty are anathema" to them, and PDWs are likely to supply insights that—in combination with other intelligence—helps groups exert more "predictability and control" over operations and their environment.[65] In turn, fighters can better mitigate "unforeseen circumstances" and craft more effective operations and internal processes, increasing their chances of success.[66] As PIRA operative Brendan Hughes later remarked, "[W]ithout intelligence forget about it…Intelligence is the heartbeat of the war."[67] PDWs

may therefore disclose information that has strategic and tactical benefits for nonstate groups, including efforts to protect communications, target individuals, and undertake surveillance.

Strategic-Level Benefits

Nonstate groups are likely to combine sensitive information disclosed by PDWs with data gleaned from government publications, declassified documents, scholarly works, media stories, legal cases, and a group's own experiences to generate exploitable and decisive insights regarding U.S. and Western military and intelligence capabilities. Most armed groups probably can easily translate documents and accompanying media stories, due to the number of foreign students and native-born individuals in the United States and the West who have joined armed groups or who participate in Internet-based propaganda efforts.[68] Moreover, armed groups—like the Libyan fighters in the opening vignette—may be able to tap growing Internet access to "crowd source" intelligence needs, such as translation, compilation, and analysis of leaked information, using members of diaspora populations and ideological supporters outside war zones.[69]

This potential intelligence capability may provide an armed group with a more comprehensive assessment of adversarial threats, including the capabilities of U.S. and Western military, intelligence, and law enforcement agencies, intelligence gaps, and governmental tensions that hamper responses. At the same time, PDW collections of leaked documents, such as the Afghanistan and Iraq War materials published by WikiLeaks, have lasting relevancy as documentary resources that help inform a group's strategic-level thinking and decision making. Considering insurgents pursued a conventional strategy in 32 percent of insurgencies since 1944, or fifty of 156

campaigns, such information may become more valuable to nonstate groups in the near term, given the apparent ebbing of U.S. power after over a decade of war.[70] The collapse of Cold War-era power blocs in the 1990s, for example, encouraged 48 percent of rebel groups to use conventional warfare over guerrilla tactics, more than at any other time before or since, according to one academic study.[71]

Extremists also may indirectly derive strategic-level benefits, due to the potential chilling effects of PDW-based revelations on U.S. and Western information-sharing and intelligence collection efforts. Chelsea Manning, the source of the WikiLeaks disclosures, and Edward Snowden were able to leak large amounts of sensitive information, in part, due to the current "need-to-share" paradigm among U.S. intelligence and security agencies.[72] In response to Congressional criticism regarding information hoarding and failure to "connect the dots" after the 9/11 attacks, U.S. intelligence and security organizations reversed the venerable counterintelligence principle of "need-to-know" in order to "share information broadly across bureaucratic lines and prepare analysis for the widest possible dissemination in order to prevent intelligence stovepiping."[73] As a result, Manning and Snowden had access to sensitive information that had nothing to do with their primary responsibilities.[74]

The fallout from Manning's and Snowden's unauthorized disclosures has increased the likelihood that foreign intelligence services "may wish to distance themselves from mutually beneficial cooperative partnerships…with the U.S. government," potentially hampering efforts to collect intelligence on and quickly respond to armed groups. Germany, for example, has already has scaled back its intelligence relationships with the United States and the United Kingdom due these PDW-related

leaks.[75] At a more tactical level, the leaks probably have further complicated the already-nuanced process of U.S. information-gathering and intelligence-collection from human sources. Foreign diplomats and government officials "will think twice about sharing frank thoughts with their U.S. counterparts if they think what they say will be online tomorrow," while current and future human intelligence sources—particularly those at risk to harm if exposed—will need constant reassurance that the information they provide "won't endanger them in the next tranche of leaked information."[76]

Communications Security

Due to Snowden's disclosures, nonstate groups are now probably reviewing PDWs for the latest information regarding U.S. signals intelligence collection. Armed groups seek to protect communications against adversarial collection to ensure operational success and maintain internal cohesion—increasing a group's chances of long-term survival. Al-Qa'ida operational doctrine warns fighters that the "biggest thing that destroys organizations is the issue of communications (wire, wireless, direct, indirect). Therefore, one must pay attention to this problem and plan for this, keeping up with technological developments related to the means of communication."[77] Accordingly, PDWs like Bruce Schneier's personal website, which is compiling and explaining the technical collection tools and programs exposed by Snowden, probably are instrumental to these efforts.[78] Former NSA officials indicate ISIS has exploited Snowden's disclosures—including a leaked NSA report detailing how it electronically surveilled former bin Ladin confidant Hassan Ghul prior to his death in 2012—to learn "what types of communication to avoid or how to make them more secure."[79]

Targeting Individuals

PDWs are potentially a significant source of identity information that armed groups could use to harm U.S. and Western military, diplomatic, intelligence personnel. Cryptocomb is especially troubling in this regard due to its efforts to profile alleged CIA personnel. The site has compiled extensive dossiers on some individuals, including photographs, addresses, including maps and street-level views of residences, past job titles, information about family members, and other personal details.[80] There is no evidence Cryptocomb supports violent groups, but the site's efforts resemble intelligence requirements extremists may use to plan assassinations. Al-Qa'ida operational doctrine, for example, instructs fighters to pinpoint a target by collecting

> A. Personal information: his name, age, his photograph, his home address, his car (the make, color, license plate number, model), his daily routine…his weekly routine, where he spends his vacations…
>
> C. Information about the house and its site (the exact address, the part of town, the block where the house is, the house or the building itself, the floor, the apartment, the room).[81]

To date there is no evidence that extremists have used Cryptocomb's or any other PDW's information to attack an official, but this risk is not without precedent. In 1975, Greek terrorists assassinated Richard Welch, the CIA station chief in Athens, Greece, after the Greek press published both his name—initially exposed in *Counter Spy*, a left-wing U.S. magazine—and address.[82] Should extremists wish to target the individuals on Cryptocomb, the site has given them strong leads. Sadly, these individuals, whether accurately identified or not, probably remain at risk for harassment or violence because Cryptocomb's information cannot be wholly expunged from the Internet, even if the site removes its dossiers.

Similarly, extremists might identify spies and informants within a group by gleaning clues from leaked documents. For example, after the WikiLeaks revelations in 2010, a Taliban spokesman warned, “We will investigate through our own secret service whether the people mentioned [in Afghanistan-related documents] are really spies working for the US. If they are US spies, then we know how to punish them.”[83] Subsequently, the group claimed to have uncovered and executed a spy in Kandahar on the basis of WikiLeaks information, but this claim has been disputed.[84] Whether other armed groups have undertaken similar investigations and reprisals is unclear.

Adjunct Surveillance

Sensitive government information disclosed by PDWs also potentially benefits extremist operational planning, particularly in the initial stages. Armed groups are increasingly using the Internet to gather open-source intelligence on targets, because it provides both the cyberspace equivalent of discreet surveillance and a forum to communicate findings.[85] Easily-searched PDW collections of leaked and declassified government documents, maps and images of sensitive sites, including satellite imagery, and other materials potentially provide extremists with significant seed material for operations. In December 2010, WikiLeaks arguably made the most notorious disclosure in this regard after publishing a classified U.S. State Department “list of worldwide critical infrastructure,” including hydroelectric sites, pharmaceutical plants, and undersea cable locations.[86] Some sites probably were already known to armed groups, but publication of the list revealed greater insight into U.S. strategic concerns, as well as exposed locations extremists may not have previously identified or thought important.

Recommendations

Two high-profile leaks of sensitive U.S. government information in three years suggest that additional, and just as sizable, unauthorized disclosures are probable, particularly as more sensitive information is now shared for homeland security purposes and as more government data is released online.[87] Uniformly implementing information controls across this enterprise to mitigate leaks will be a challenge. Nonetheless, initiatives are already underway.[88] Further options to consider include:

- **Seek comprehensive legislation regarding leaks**. A recent RAND study notes that U.S. legislators and officials are more open to reforming U.S. statues regarding leaks and espionage.[89] Accordingly, U.S. national security agencies should work with Congress and the White House to craft "new provisions distinct from the espionage laws" for those who engage in unauthorized disclosures, as well as "carefully tailored" civil sanctions regarding the publication of classified information "with gross negligence or reckless disregard" for national security.[90]
- **Tailor "need to share" to "need for mission."** Government personnel should have access to all mission-specific information—but no more. Chelsea Manning, for example, should have been able to access only Iraq-related State Department documents, not the entire database. Likewise, access to sensitive information should be rescinded, as appropriate, once personnel move to a new account or mission.
- **Encrypt.** U.S. Government computer systems, including unclassified systems, should employ multiple layers of encryption to protect data.[91] If

improperly removed, materials would be unreadable without decryption, delaying, if not completely neutralizing, the potential impact of a leak.

- **Utilize technology.** Similarly, U.S. Government agencies should leverage computer technologies to educate personnel about leaking, flag suspicious computer-related activity, and investigate leaks after they have occurred. RAND notes that these tools are available, or can be readily adapted, and should be incorporated into new systems like the Joint Information Environment before they are fielded.[92]

Conclusion

To date, there is no evidence linking information published by PDWs to an extremist attack, but this threat is almost certain to grow as Internet access expands globally and brings improperly disclosed materials into the reach of more armed groups. Moreover, the notoriety of WikiLeaks and Edward Snowden probably has further inspired activists and created new supporters, who will use innovations in encryption and anonymizing software—some of which has been created in response to Snowden's leaks—to engage in leaking and protect leakers and self-proclaimed whistleblowers.[93] Indeed, the PDW phenomenon "may well make the first half of the twenty-first century the age of the whistleblower."[94] Therefore, robust governmental information controls are now critical to mitigating the threat posed by PDWs, particularly given that at least some of these activists have no qualms about exposing the identities of U.S. intelligence and security personnel, or U.S. intelligence sources. Left unchallenged, this type of PDW activity fundamentally threatens the ability of the United States to counter violent nonstate groups.

Endnotes

[1] John Pollock, “People Power 2.0: How civilians helped win the Libyan information war,” *Technology Review*, May-June 2012, 63-64.

[2] Internet users in the developing world accounted for nearly two-thirds of the world’s Internet users in 2014. Likewise, 55 percent of the world’s 2.3 billion mobile-broadband subscribers in 2014 lived in the developing world. This trend continues to grow. See, “Internet well on way to 3 billion users, UN telecom agency reports,” *M2 PressWire*, May 6, 2014; “Cisco Visual Networking Index Predicts Annual Internet Traffic to Grow More Than 20 Percent (reaching 1.6 Zettabytes) by 2018; More Traffic Will Traverse Global Networks in 2018 Than All Prior ‘Internet Years’ Combined; Ultra-HD/4K Adoption and M2M Technologies Including Smart Cars Among Key Growth Drivers,” *M2 PressWire*, 10 June 2014.

[3] Christopher M. Ford, “Of Shoes and Sites: Globalization and Insurgency,” *Military Review* 87, no. 3 (May-June 2007): 88; Timothy L. Thomas, “Al Qaeda and the Internet: The Danger of ‘Cyberplanning,’” *Parameters* 33, no. 1 (Spring 2003): 112-123.

[4] Wendy H. Wong and Peter A. Brown, “E-Bandits in Global Activism: WikiLeaks, Anonymous, and the Politics of No One,” *Perspectives on Politics* 11, no. 4 (December 2013): 1018; Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: Penguin Press, 2011), 171

[5] Wong and Brown, “E-Bandits in Global Activism,” 1018.

[6] Academic books, chapters, and journal articles on these topics now probably run into the tens of thousands in English alone. See Paul J. Smith, *The Terrorism Ahead: Confronting Transnational Violence in the Twenty-first Century* (Armonk, NY: M.E. Sharpe, Inc., 2008), 73-75; Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: United States Institute of Peace Press, 2006), 111-145, 193-196; Wael Adhami, “The strategic importance of the Internet for armed insurgent groups in modern warfare,” *International Review of the Red Cross* 89, no. 868 (December 2007): 857-878; Steven Metz, “The Internet, New Media, and the Evolution of Insurgency,” *Parameters* 42, no. 3 (Autumn 2012): 80-90; Thomas, “Al Qaeda and the Internet,” 114, 118.

[7] Manuel R. Torres-Soriano, “The Vulnerabilities of Online Terrorism,” *Studies in Conflict & Terrorism* 35, no. 4 (2012): 263-277.

[8] David C. Benson, “Why the Internet Is Not Increasing Terrorism,” *Security Studies* 23, no. 2 (2014): 295. Benson reviews al-Qa’ida attacks from 1995-2011, but does not examine the efforts of other groups like Hezbollah.

[9] William Rosenau, “Understanding Insurgent Intelligence Operations,” *Marine Corps University Journal* 2, no. 1 (Spring 2011): 1. See also Blake W. Mobley, *Terrorism and Counterintelligence: How Terrorist Groups Elude Detection* (New York: Columbia University Press, 2012).

[10] Weimann, *Terror on the Internet*, 113.

[11] Jerrold M. Post ed., *Military Studies in the Jihad Against the Tyrants: The Al-Qaeda Training Manual* (Maxwell Air Force Base, AL: USAF Counterproliferation Center, n.d.), 87-88.

[12] Norman Cigar trans., *Al-Qa'ida's Doctrine for Insurgency: 'Abd Al-'Aziz Al-Muqrin's A Practical Course for Guerilla War* (Washington, DC: Quicksilver Books, Inc., 2009), 122.

[13] Alasdair Roberts, "The WikiLeaks Illusion: WikiLeaks' tsunami of revelations from U.S. government sources last year did not change the world, but it did change WikiLeaks," *Wilson Quarterly* 35, no. 3 (Summer 2011): 17.

[14] Ibid, 18.

[15] Erik J. Dahl, "Finding Bin Laden: Lessons for a New American Way of Intelligence," *Political Science Quarterly* 129, no. 2 (Summer 2014): 195.

[16] Stephanie Strom, "Pentagon Sees a Threat From Online Muckrakers," *New York Times*, March 18, 2010.

[17] Adam Goldman and Lara Jakes, "Encryption helps terrorists evade U.S. Threat that closed embassies was discussed in chat room" *St. Louis Post-Dispatch*, August 15, 2013.

[18] Steven Swinford, "Spy chief: Facebook is helping terrorists; Technology giants are in denial over their responsibility, says new head of GCHQ," *The Daily Telegraph*, November 4, 2014.

[19] Ezzeldeen Khalil, "Cloud cover - Jihadists' use of anonymizing internet security," *Jane's Intelligence Review*, February 18, 2014, 2.

[20] James B. Bruce, "How Leaks of Classified Intelligence Help U.S. Adversaries: Implications for Laws and Secrecy," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, ed. Roger Z. George and Robert D. Kline (Washington, DC: National Defense University Press, 2004), 401.

[21] Ibid.

[22] Ibid., 399.

[23] Ibid.

[24] Steven Swinford, Michael Smith, and Stephen Grey, "Freedom Fighter or Information Terrorist?," *National Edition*, August 1, 2010, 13.

[25] Wong and Brown, "E-Bandits in Global Activism," 1018.

[26] Eric Hughes, "A Cypherpunk's Manifesto," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge, MA: The MIT Press, 2001), 82.

[27] Julian Assange with Jacob Appelbaum, Andy Müller-Maguhn, and Jérémie Zimmermann, *Cypherpunks: Freedom and the Future of the Internet* (New York: OR Books, 2012), 5.

[28] James Jay Carafano, *Wiki at War: Conflict in a Socially Networked World* (College Station, TX: Texas A&M University Press, 2012), 202; Brenner, *America the Vulnerable*, 171;

Charlie Beckett with James Hall, *WikiLeaks: News in the Networked Era* (Cambridge, UK: Polity Press, 2012), 156-157; Rahul Sagar, *Secrets and Leaks: The Dilemma of State Secrecy* (Princeton, NJ: Princeton University Press, 2013), 178-179.

[29] Beckett, *WikiLeaks*, 120.

[30] Lee Rainie and Barry Wellman, *Networked: The New Social Operating System* (Cambridge, MA: MIT Press, 2012), 240.

[31] Jascha Hoffman, "Sousveillance," *New York Times Magazine*, December 10, 2006, http://www.nytimes.com/2006/12/10/magazine/10section3b.t-3.html?_r=0 (accessed November 28, 2014).

[32] Rainie and Wellman, *Networked*, 240.

[33] Carafano, *Wiki at War*, 202; Neville Bolt, "The Leak Before the Storm: What WikiLeaks Tells US About Modern Communication," *The RUSI Journal* 155, no. 4 (August/September 2010): 48.

[34] Rainie and Wellman, *Networked*, 241.

[35] David Leigh and Luke Harding, *WikiLeaks: Inside Julian Assange's War on Secrecy* (New York: PublicAffairs, 2011), 51-56.

[36] Andy Greenberg, *This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hacktivists Aim to Free the World's Information* (New York: Dutton, 2012), 318-319.

[37] Manuel R. Torres-Soriano, "The Hidden Face of Jihadist Internet Forum Management: The Case of Ansar Al Mujahideen," *Terrorism and Political Violence* (2014): 1.

[38] Wong and Brown, "E-Bandits in Global Activism," 1019.

[39] Peter Maass, "Snowden's People," *New York Times Magazine* (August 18, 2013): 22-29, 49; Anthony Faiola, "WikiLeaks aids Snowden on the run," *Washington Post*, June 24, 2013, http://search.proquest.com/docview/1370504061?accountid=4444; Colin Freeze, "There are so Many Stories left," *The Globe and Mail*, October 20, 2014, http://search.proquest.com/docview/1614723083?accountid=4444.

[40] Bolt, "The Leak Before the Storm," 48; Roberts, "The WikiLeaks Illusion," 18-19; Sagar, *Secrets and Leaks*, 178-179.

[41] Roberts, "The WikiLeaks Illusion," 18.

[42] Ibid, 18-19.

[43] Bolt, "The Leak Before the Storm," 48-49.

[44] Sagar, *Secrets and Leaks*, 178.

[45] Bolt, "The Leak Before the Storm," 48.

[46] *Wayback Machine Home Page*, www.archive.org (accessed November 30, 2014).

[47] Rainie and Wellman, *Networked*, 241.

[48] Brenner, *America the Vulnerable*, 170.

[49] Quoted in Gaetano Joe Ilardi, "IRA operational intelligence: the heartbeat of the war," *Small Wars & Insurgencies* 21, no. 2 (June 2010): 335.

[50] Carafano, *Wiki at War*, 202-203.

[51] Beckett, *WikiLeaks*, 19.

[52] Beckett, *WikiLeaks*, 115-116, 121; Greenberg, *This Machine Kills Secrets*, 229, 318-319; *GlobaLeaks Home Page*, www.globaleaks.org (accessed November 22, 2014). Other disruptive PDWs noted by Beckett and Greenberg include: BaltiLeaks, BritiLeaks, BrusselsLeaks, Corporate Leaks, CrowdLeaks, EnviroLeaks, FrenchLeaks, GlobaLeaks, JumboLeaks (a campus watchdog at Tufts University), Indoleaks, IrishLeaks, IsraeliLeaks, JamiiForums, Jumbo Leaks, KHLeaks, LeakyMails, Localeaks, MapleLeaks, MurdochLeaks, Office Leaks, Porn WikiLeaks, PinoyLeaks, PirateLeaks, QuebecLeaks, RuLeaks, ScienceLeaks, ThaiLeaks, TradeLeaks, and UniLeaks. Some of these sites may no longer be operating.

[53] Greenberg, *This Machine Kills Secrets*, 100-101.

[54] *Cryptocomb Home Page*, www.cryptocomb.org (accessed November 22, 2014).

[55] Russ Kick, "From Their Vaults to Your Desktop," *The Village Voice*, May 16, 2000, 44-45; Laura Gordon-Murnane, "Shhh!!: Keeping Current on Government Secrecy," *Searcher*, January 2006, 35-47. Gordon-Murnane offers an extensive list of government transparency sites, including BushSecrecy.org (bushsecrecy.org), Center for Democracy and Technology (cdt.org), Coalition of Journalists for Open Government (cjog.net), Freedom of Information Clearinghouse (citizen.org), MemoryHole (thememoryhole.org), National Security Whistleblowers Coalition (nswbc.org), OMB Watch (ombwatch.org), Project on Government Oversight (pogo.org), OpenTheGovernment.org (openthegovernment.org), Common Cause (commoncause.org), Freedom of Information Center (missouri.edu), FreedomInfo.org (freedominfo.org), Government Accountability Program (whistleblower.org), and Judicial Watch (judicialwatch.org). Many of these same sites operate ancillary websites and blogs providing updates about declassified U.S. government materials and whistleblowing-related news.

[56] Gordon-Murnane, "Shhh!!,"38.

[57] Ibid.

[58] Ibid., 36-38.

[59] Ibid., 40-41, 43.

[60] Beckett, *WikiLeaks*, 127-128; Sagar, *Secrets and Leaks*, 165.

[61] Beckett, *WikiLeaks*, 127.

[62] Ibid.

[63] *Bruce Schneier Home Page*, www.schneier.com (accessed November 22, 2014).

[64] Peter Grier, "Soldier arrested in WikiLeaks classified Iraq video case" *Christian Science Monitor*, June 7, 2010, 7; Maria Glod, "Former FBI employee sentenced in classified leak," *Washington Post*, May 25, 2010.

[65] Ilardi, "IRA operational intelligence," 347; Gaetano Joe Ilardi, "Irish Republican Army Counterintelligence," *International Journal of Intelligence and Counterintelligence*, 23, no. 1 (2009): 2.

[66] Ilardi, "IRA operational intelligence," 347.

[67] Quoted in Ibid., 331.

[68] David V. Gioe, "Tinker, Tailor, Leaker, Spy," *The National Interest*, no. 129 (January-February 2014): 55.

[69] Pollock, "People Power 2.0," 63-71.

[70] Seth G. Jones and Patrick B. Johnston, "The Future of Insurgency," *Studies in Conflict & Terrorism* 36, no. 1 (2013): 6.

[71] Ibid.

[72] Gioe, "Tinker, Tailor, Leaker, Spy," 51.

[73] Ibid.

[74] Ibid.

[75] Ibid., 55-56.

[76] Ibid., 53-55.

[77] Cigar, *Al-Qa'ida's Doctrine for Insurgency*, 123.

[78] *Bruce Schneier Home Page*, www.schneier.com (accessed November 22, 2014).

[79] Rowan Scarborough, "Islamic State using leaked Snowden info to evade U.S. intelligence: Disclosures from classified documents help terrorist group's militants avoid detection," *Washington Times*, September 4, 2014, http://www.washingtontimes.com/news/2014/sep/4/islamic-state-using-edward-snowden-leaks-to-evade-/?page=all#pagebreak (accessed September 4, 2014).

[80] *Cryptocomb Home Page*, www.cryptocomb.org (accessed November 22, 2014).

[81] Cigar, *Al-Qa'ida's Doctrine for Insurgency*, 142-143.

[82] John Crewdson, "The murder that sparked Identities Protection Act," *Chicago Tribune*, March 12, 2006, http://articles.chicagotribune.com/2006-03-12/news/0603120383_1_spy-then-cia-director-william-colby-intelligence-identities-protection-act (accessed December 1, 2014); Mark Landler, "Greek Court Convicts 15 in 27-Year-Old Terror Group," *New York Times*, December 9, 2003, http://www.nytimes.com/2003/12/09/world/greek-court-convicts-15-in-27-year-old-terror-group.html (accessed December 1, 2014); David Wise, "The Cold War is Over,

but for Spies the Risk of Death Remains the Same CIA: Freddie Woodruff, Slain on a Mission to Help an Old U.S. Ally in the Former Soviet Union, was the 57th Agent to Die. An Unusual Trip by our Top Spy," *Los Angeles Times*, August 15, 1993. http://search.proquest.com/docview/281978836?accountid=4444.

[83] Swinford, Smith, and Grey, "Freedom Fighter or Information Terrorist?,"13.

[84] Gioe, "Tinker, Tailor, Leaker, Spy," 55.

[85] Kevin A. O'Brien, "Assessing Hostile Reconnaissance and Terrorist Intelligence Activities: The Case for a Counter Strategy," *The RUSI Journal* 153, no. 5 (October 2008): 35.

[86] Brenner, *America the Vulnerable*, 174.

[87] Carafano, *Wiki at War*, 202.

[88] See James B. Bruce and W. George Jameson, *Fixing Leaks: Assessing the Department of Defense's Approach to Preventing and Deterring Unauthorized Disclosures* (Santa Monica, CA: The RAND Corporation, 2013). Bruce and Jameson provide an unclassified review and further recommendations for the Office of the Secretary of Defense regarding the implementation of its anti-leak efforts enacted in the wake of Manning's and Snowden's leaks.

[89] Ibid., 34.

[90] Ibid.

[91] Ibid., 33.

[92] Ibid., 33-34.

[93] Greenberg, *This Machine Kills Secrets*, 316; Swinford, "Spy chief."

[94] Carafano, *Wiki at War*, 202.