America is 'dropping cyberbombs'—but how do they work?

May 11 2016, by Richard Forno And Anupam Joshi, University Of Maryland, Baltimore County

Inside the U.S. Army's Cyber Operations Center at Fort Gordon, Georgia. Credit: Army-Cyber/flickr

Recently, United States Deputy Defense Secretary Robert Work publicly confirmed that the Pentagon's Cyber Command was "dropping cyberbombs," taking its ongoing battle against the Islamic State group into the online world. Other American officials, including President Barack Obama, have discussed offensive cyber activities, too.

The American public has only glimpsed the country's alleged cyberattack abilities. In 2012 The New York Times revealed the first digital weapon, the Stuxnet attack against Iran's nuclear program. In 2013, former NSA contractor Edward Snowden released a classified presidential directive outlining America's approach to conducting Internet-based warfare.

The terms "cyberbomb" and "cyberweapon" create a simplistic, if not also sensational, frame of reference for the public. Real military or intelligence cyber activities are less exaggerated but much more complex. The most basic types are off-the-shelf commercial products used by companies and security consultants to test system and network security. The most advanced are specialized proprietary systems made for exclusive – and often classified – use by the defense, intelligence and law enforcement communities.

So what exactly are these "cyberbombs" America is "dropping" in the Middle East? The country's actual cyber capabilities are classified; we, as researchers, are limited by what has been made public. Monitoring books, reports, news events and congressional testimony is not enough to separate fact from fiction. However, we can analyze the underlying technologies and look at the global strategic considerations of those seeking to wage cyber warfare. That work allows us to offer ideas about cyber weapons and how they might be used.

A collection of capabilities

A "cyberbomb" is not a single weapon. Rather, cyberweapons are collections of computer hardware and software, with the knowledge of their potential uses against online threats. Although frequently used against Internet targets such as websites and forums, these tools can have real-world effects, too. Cyberattacks have disrupted cellphone networks and tricked computers controlling nuclear centrifuges into functioning differently from how they report their status to human operators. A

simulated attack has shown how an enemy can remotely disrupt electric power generators.

The process of identifying potential targets, selecting them and planning "cyberbomb" attacks includes not only technological experts but military strategists, researchers, policy analysts, lawyers and others across the military-industrial complex. These groups constantly analyze technology to develop the latest cyber weapons and tactics. They also must ensure the use of a given "cyberbomb" aligns with national interests, and follows national and international laws and treaties.

For example, as part of their counterterrorism efforts, electronic intelligence services (such as the American NSA and British GCHQ) routinely collect items like real names, user IDs, network addresses, Internet server names, online discussion histories and text messages from across the Internet. Gathering and analyzing these data could use both classified and unclassified methods. The agencies could also conduct advanced Google searches or mine The Internet Archive's Wayback Machine. This information can be linked with other data to help identify physical locations of target computers or people. Analysts can also observe interconnections between people and infer the types and strengths of those relationships.

This information can clue intelligence analysts in to the existence of previously undiscovered potential Internet targets. These can include virtual meeting places, methods of secure communications, types of phones or computers favored by the enemy, preferred network providers or vulnerabilities in their IT infrastructures. In some cases, cyberattacks need to be coordinated with spies or covert agents who must carry out physical aspects of the plan, especially when the electronic target of a "cyberbomb" is hard to reach – such as the computers inside the Iranian nuclear facility targeted by the Stuxnet worm.

Cyberattack purposes can vary widely. Sometimes, a government entity wants to simply monitor activity on a specific computer system in hopes of gaining additional intelligence. Other times, the goal is to place a hidden "backdoor" allowing the agency to secretly take control of a system. In some cases, a target computer will be attacked with the intent of disabling it or preventing future use by adversaries. When considering that kind of activity, planners must decide whether it's better to leave a site functional so future intelligence can be collected over the long term, or to shut it down and prevent an adversary from using it in the near term.

Although not strictly a "cyber" attack, "cyberbombing" also might entail the use of decades-old electronic warfare techniques that broadcast electromagnetic energy to (among other things) disrupt an adversary's wireless communications capabilities or computer controls. Other "cyberbombing" techniques include modifying or creating false images on an enemy's radar screens ahead of an air attack, such as how Israel compromised Syria's air defense systems in 2007. These may be done on their own or to support more traditional military operations.

Finally, using an electromagnetic pulse (EMP) weapon to disrupt and/or disable all electronic circuits over a wide area – such as a city – could be considered the "Mother of All Cyber Bombs." As such, its effect would be felt both by enemy forces and local (likely) noncombatant citizens, all of whom suddenly would be unable to obtain fresh water and electricity, and find their local hospitals, banks and electronic items ranging from cars to coffee pots unable to function. Depending on the heat and blast from the bomb's detonation, some people might not notice – though those dependent on electronic medical devices like pacemakers probably would feel effects immediately. EMP is commonly associated with nuclear weapons, but even using nonnuclear EMP devices in a populated area would presumably cause enough "collateral damage" that it would violate international laws.

Fighting against nongovernment groups

In addition to the above techniques, and particularly when fighting opponents that are not foreign governments – such as ISIS – a unique type of "cyberbombing" seeks to target the online personas of terror group leaders. In this type of attack, one goal may be to tarnish their online reputations, such as publishing manipulated images that would embarrass them. Or, cyber weaponry may be used to gain access to systems that could be used to issue conflicting statements or incorrect orders to the enemy.

These types of "cyberbombs" can create psychological damage and distress in terrorist networks and help disrupt them over time. The United Kingdom's JTRIG (Joint Threat Research Intelligence Group) within GCHQ specializes in these tactics. Presumably similar capabilities exist in other countries.

Making cyberwar public

Until recently, few nations publicly admitted planning or even thinking about waging offensive warfare on the Internet. For those that do, the exact process of planning a digital warfare campaign remains a highly guarded military and diplomatic secret.

The only people announcing their cyberattacks were assorted hacktivist groups such as Anonymous and the self-proclaimed "Cyber-Caliphate" supporting ISIS. By contrast, the most prominent cyber-attack waged by a nation-state (2011's Stuxnet) – allegedly attributed to the United States and Israel – was never officially acknowledged by those governments.

Cyber weapons and the policies governing their use likely will remain shrouded in secrecy. However, the recent public mentions of cyber

warfare by national leaders suggest that these capabilities are, and will remain, prominent and evolving ways to support intelligence and military operations when needed.

This article was originally published on The Conversation. *Read the* original article.

Source: The Conversation