The Rise of Hacktivism | Georgetown Journal of International Affairs

(Piracy Manifesto, Wikipedia)

The rise of the Internet and related technologies brought with it new methods and practices in all areas of human activity, including activism. Activism in particular was affected in two ways. First, new technologies gave protesters a convenient and powerful means to spread their messages and mobilize action globally. And second, the topic of this article, technological innovations gave protesters the ability to employ hacking tools to conduct cyber operations analogous to street protests and sit-ins. This blending of hacking with activism, known as “hacktivism,” has become increasingly prevalent and is now commonplace. Hacktivism is challenging international affairs, not only because it transcends borders, but also because it has become an instrument of national power.

Early History

Hacktivism emerged in the late 1980s at a time when hacking for fun and profit were becoming noticeable threats. Initially it took the form of computer viruses and worms that spread messages of protest. A good example of early hacktivism is “Worms Against Nuclear Killers (WANK),” a computer worm that anti-nuclear activists in Australia unleashed into the networks of the National Aeronautics and Space Administration and the US Department of Energy in 1989 to protest the launch of a shuttle which carried radioactive plutonium.

By the mid-1990s, denial of service (DoS) attacks had been added to the hacktivist's toolbox, usually taking the form of message or traffic floods. In 1994, journalist Joshua Quittner lost access to his e-mail after thousands of messages slamming "capitalistic pig" corporations swamped his inbox, and a group called itself "The Zippies" flooded e-mail accounts in the United Kingdom with traffic to protest a bill that would have outlawed outdoor dance festivals. Then in 1995, an international group called Strano Network organized a one-hour "Net'strike" against French government websites to protest nuclear and social policies. At the designated time, participants visited the target websites and hit the "reload" button over and over in an attempt to tie up traffic to the sites.

In 1996, hacktivists started attacking websites and replacing their home pages with messages of protest. In one of the first web defacements of this nature, someone changed the homepage of the United States Department of Justice website to read "Department of Injustice" and display pornographic images in protest of the Communications Decency Act (which was later ruled unconstitutional).

The term "hacktivism" was coined that same year by the Cult of the Dead Cow (cDc), an organization which also gave birth to Hacktivismo, an international group of hackers and other protesters dedicated to the advancement of human rights. Rather than launching cyber-attacks, Hacktivismo used their programming skills to develop software tools to support free speech and privacy. They decried the use of DoS attacks and web defacements as being antithetical to free speech.

The media picked up the term "hacktivism" during the 1998-1999 Kosovo conflict when activists from around the world launched DoS attacks and defaced or hijacked web sites to protest the war and the countries engaged in it. The American-based group Team Spl0it wrote "stop the war" on a US Federal Aviation Authority site; the Russian Hackers Union wrote "stop terrorist aggression against Jugoslavia on a US Navy site;" and the Serb Black Hand Group (Crna Ruka) conducted DoS attacks against computers owned by the North Atlantic Treaty Organization (NATO) and other entities. Even Chinese hacktivists got involved, defacing US websites and launching DoS attacks following the accidental bombing of their embassy in Belgrade.

That late 90s also saw the birth of the Electronic Disturbance Theater (EDT), a group of New York-based activists that blended radical politics with software and art. EDT developed the concept of electronic civil disobedience along with a software tool called FloodNet for conducting what they called "virtual sit-ins." The tool essentially automated the manual reloads used in Strano's "Net'strikes." EDT's initial actions aimed to support the Mexican Zapatistas by flooding Mexican and US-government sites in 1998, but they later expanded their goals and targets to protest policies relating to globalization and capitalism.

Several other hacking groups also emerged and carried out widely publicized attacks in the late 1990s. The Internet Black Tigers flooded Sri Lanken embassies with 800 e-mails a day for two weeks in 1997 in what they called "suicide e-mail bombings." Milw0rm defaced the website of India's Bhabha Atomic Research Center to protest India's nuclear weapons testing in 1998. The UK-based Electrohippies organized a major web sit-in against the World Trade Organization in 1999. Finally, an alliance of

Chinese hacker groups began conducting cyber-attacks in 1998 to support their homeland. Chinese attacks in response to the bombing of the embassy in Belgrade were one example of the alliance's national attacks.

The Hacktivism e-mail distribution list was also started during this period, characterizing itself as "the fusion of hacking and activism." In 1999, the list was used to organize Jam Echelon Day, a protest event against the Echelon global surveillance system operated by the United States, the United Kingdom, Canada, Australia, and New Zealand. On the appointed day, protesters were asked to flood email systems with messages containing words that were likely o be picked up by Echelon's keyword filters in order to overload the system.

Becoming Commonplace

By the turn of the century, hacktivism had become a common means of protest. It accompanied military and international conflicts as well as street protests. The intelligence firm iDefense reported that during the early months of the second intifada that erupted between Israel and the Palestinians in September 2000, over 30 pro-Palestinian and 10 pro-Israeli hacktivists and hacktivist groups conducted cyber-attacks. The following year, after a mid-air collision between a US intelligence aircraft and a Chinese Navy jet on April 1, iDefense reported seeing over 1,400 web defacements from over 140 hacktivist groups, along with numerous DoS attacks. The web defacements by pro-Chinese hacktivists, including the Honker Union of China and China Eagle, vastly outnumbered those by pro-US hacktivists. Then later that year, the September 2001 terrorist attacks by al-Qaeda and the start of Operation Enduring Freedom gave birth to such groups as the Young Intelligent Hackers Against Terrorism, which aimed to stop the financing of terrorists, and a coalition of Pakistani hacker groups that called itself the Al-Qaeda Alliance Online.

Despite its prevalence for over two decades, hacktivism is frequently associated with the actions of Anonymous, an unorganized collective of activists and hackers known for wearing Guy Fawkes masks and their use of an image of a man in a suit with a "?" for his head. Anonymous emerged in 2003, but it did not enter the public spotlight until 2008 when the group launched Project Chanology to protest efforts by the Church of Scientology to censor a video of the actor Tom Cruise praising the church. Since then, Anonymous, along with its related offshoots and regional and local affiliates have been responsible for thousands of cyber-attacks worldwide. They have conducted operations against governments, companies, churches, terrorists, drug dealers, and pedophiles. They have also partnered with other hacktivists in large-scale operations. Since 2013, Anonymous has participated in yearly operations against Israel on April 7 to protest Israeli actions against the Palestinian people. In 2014, the operation, dubbed #OpIsraeliBirthday, involved over twenty other groups, including AnonGhost; the Syrian Electronic Army (SEA), the Afghan Cyber Army, the Gaza Hacker Team, the Izz ad-Din al-Qassam Cyber Fighters, Anonymous Syria, Anonymous Jordan, and Anonymous Lebanon. Cyber operations against Israel have also generated counter-actions from groups such as the Israeli Elite Force.

Today there are thousands of hacktivist groups worldwide supporting practically every cause imaginable.

Some of these groups associate themselves with a particular country (e.g., Anonymous Syria), government (e.g., SEA supporting the Assad regime), or other entity (e.g., Cyber Caliphate supporting the Islamic State), while others express no particular allegiances (e.g., Anonymous). Most do not explicitly call themselves “hacktivists.” The term is more commonly used by researchers, journalists, and cyber security professionals trying to distinguish different types of threat actors in cyberspace.

In addition to conducting DoS attacks, and defacing and hijacking websites, hacktivists take over Twitter accounts and Facebook pages, and they steal and disclose sensitive and personal information from the systems that they penetrate. They also make extensive use of social media to publicize their actions and generate support. Many groups have their own Twitter accounts and Facebook pages, and operations such as #OpIsraeliBirthday are given hashtags and announced on Twitter. Until it was taken down, #OpIsraeliBirthday even had its own domain and website.

There are several reasons why hacktivism has become so popular. First, it is a relatively easy to conduct, low-cost operation. People with little or no technical skill can use free, user-friendly tools such as Anonymous’ Low (or High) Orbit Ion Cannon to launch DoS attacks. Second, unlike participating in a street demonstration, hacktivism poses little risk to protesters. Most cases are never even investigated by law enforcement agencies. Third, internet activism supports remote actions. Hacktivists can take on distant causes without the need to travel anywhere. Fourth, it enables both individual actions and large-scale distributed efforts. Persons of a common nationality or united by a common cause, for example, can join together whether residing in their homeland or in a foreign country. Fifth, the effects of hacktivism are often visible, such as when websites are defaced to display protesters’ messages or shut down from DoS attacks, or when protesters report their actions via Twitter or Facebook. Some hacktivists have even made videos of screenshots showing the effects of their DoS attacks.

Most of the cyber-attacks performed by hacktivists are illegal under domestic crime statutes. Few cases, however, reach the point of prosecution, in part because the damages are usually minor. Defaced web sites are easily restored, and DoS attacks often have little or no impact. Moreover, attribution can be difficult. Even though entities such as Anonymous claim credit for their actions, they do not reveal the legal identities of the people behind the code names. Unless damages are significant, law enforcement agencies are unlikely to start an investigation. Still, in a few cases, such as the one against members of the Anonymous offshoot LulzSec, hacktivists have been identified and prosecuted for violating cybercrime laws.

Challenges in International Relations

The rise of hacktivism has brought with it two related challenges in international relations. The first concerns the responsibility of states in prosecuting independent hacktivists that are operating on domestic soil and against targets in other countries. Although few cases of hacktivism are actively investigated, when one is, investigators in the country of the target of a cyber-attack may need help from their counterparts in the countries of origin, in order to identify and prosecute the perpetrators. This can be problematic, if the countries involved are not party to some form of mutual assistance agreement.

Even if they are, a country might refuse to cooperate. Such was the case when Russian hacktivists launched highly disruptive cyber-attacks against Estonia in 2007 to protest the relocation of a Soviet-era war memorial. Even though some of the attacks were traced back to Russia, Moscow turned down Estonia's request for help, claiming that the request was not foreseen by their mutual legal assistance treaty. The Council of Europe's Convention on Cybercrime includes requirements for mutual assistance in cybercrime investigations, but many countries, including Russia, have not signed onto it.

Recognizing the problems of mutual assistance in cybercrimes, a group of experts reporting to the Secretary-General of the United Nations in June 2013 recommended that "states should intensify cooperation against criminal or terrorist use of ICTs [Information and Communication Technologies], harmonize legal approaches as appropriate and strengthen practical collaboration between respective law enforcement and prosecutorial agencies." They further recommended that "states should seek to ensure that their territories are not used by non-State actors for unlawful use of ICTs." In 2015, the group recommended that states assist with investigating cyberattacks and cybercrime launched from their territories. The recommendations are non-binding, but show a growing sentiment for cracking down on cybercrimes and improving international cooperation.

Although mutual assistance is an issue across all areas of cybercrime, it can be aggravated in cases of hacktivism, as the governments of the countries where the hacktivists reside might sympathize with the actions of the hackers. In the case of the Estonian attacks, for example, the Russian government had voiced opposition to Estonia's relocation plans, so it was unsurprising that it did not aid the investigation. Many cases of hacktivism involve "patriotic hackers," who conduct cyber-attacks against adversaries or opponents of their own country or some other country that they identify with or support. Especially in cases where damages are relatively minor, governments may be inclined to turn a blind eye to the actions of their patriotic hackers.

The second challenge concerns states that sponsor or direct hacktivists, or that hide behind the disguise of fictitious hacktivist groups. Many people believed that the Russian government played a role in the cyber-attacks against Estonia, and then again in similar attacks against Georgia in 2008. More recently, highly damaging cyber-attacks against Sony Pictures Entertainment in late 2014 were attributed to North Korea, the apparent motivation being to stop the release of The Interview, a comedy film depicting a plot to assassinate North Korea's leader, Kim Jong-un. Although a group calling itself Guardians of Peace claimed responsibility, the U.S. government blamed North Korea and tightened sanctions against ten individuals and three agencies in the country. The United States similarly blamed Iran for cyber-attacks that were conducted in 2012 against Saudi Aramco by a group calling itself Cutting Sword of Justice. The attack protested the use of oil resources to sponsor repressive regimes. The United States also blamed Iran for cyber-attacks against major banks by a group calling itself Izz ad-Din al-Qassam Cyber Fighters. The group said they were protesting a video that mocked the Prophet Mohammad.

International Law

The UN group of experts addressed the challenge of state-sponsored or conducted cyber-attacks. They

found that international law, and in particular the Charter of the United Nations, applies to cyberspace. Specific recommendations included that "states must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts."

Even if this principle is accepted, it can be difficult to apply to state-sponsored or conducted hacktivism in practice. The reason is simply that most hacktivism does not rise to a level of force. Although the international law of armed conflict (LOAC), specifically Article 2(4) of the UN Charter, forbids member states from using or threatening to use force against other states (except in self-defense), it does not explicitly prohibit operations that do not use force.

While the UN Charter does not define "use of force," the general consensus is that the term includes acts that cause death, injury, or significant physical destruction, and that for a cyber operation to qualify as an act of force, its effects, both in terms of quality and quantity, would have to be equivalent to those of non-cyber operations that constitute the use of force. This view is reflected in the Tallinn Manual, a document prepared by an international group of experts at the invitation of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE) that applies LOAC (including both *jus in bello* and *jus ad bellum* principles) to cyber warfare. Rule 11 of the Tallinn Manual states: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."

To date, very few cyber operations have produced physical effects that are clearly equivalent to physical use of force. One example is Stuxnet, which reportedly destroyed about 1,000 centrifuges in Iran's nuclear enrichment facility at Natanz. But Stuxnet was not an act of hacktivism, and no acts of hacktivism have produced comparable physical damage. One might think that the financial losses from operations such as the one attributed to North Korea would be enough to qualify as the unlawful use of force. But those losses are likely no worse than have been imposed by economic sanctions, which are considered acceptable practice under international law.

Because most cyber-attacks, including those of hacktivists, fall below the threshold for armed conflict and the use of force, the CCDCOE launched an effort to produce a follow-on to the Tallinn Manual. Referred to as Tallinn 2.0, the group of experts will examine how international law applies to operations that are less than force and armed conflict. The group plans to consider how customary rules relating to sovereignty apply to cyber operations and the obligations of states to stop damaging cyber-attacks.

Conclusion

Hacktivism, including state-sponsored or conducted hacktivism, is likely to become an increasingly common method for voicing dissent and taking direct action against adversaries. It offers an easy and inexpensive means to make a statement and inflict harm without seriously risking prosecution under criminal law or a response under international law. Hacking gives non-state actors an attractive alternative to street protests and state actors an appealing substitute for armed attacks. It has become

not only a popular means of activism, but also an instrument of national power that is challenging international relations and international law.

Dorothy Denning

Dorothy E. Denning is Distinguished Professor of Defense Analysis at the Naval Postgraduate School. Prior to coming to NPS, she taught at Purdue University and Georgetown University, and worked in research labs at SRI International and Digital Equipment Corporation. Her teaching and research have focused on cyber security and cyber conflict. Dr. Denning is author of *Information Warfare and Security* and has testified before the U.S. Congress on encryption policy and cyber terrorism. She has received numerous awards and was inducted into the inaugural class of the National Cyber Security Hall of Fame. For more information about her and her publications, see http://faculty.nps.edu/dedennin/.

Be first to comment