The Internet War

by Nadim Kobeissi via chela - The Link *Tuesday, Oct 19 2010, 7:19pm*
international / mass media / other press

> WikiLeaks's recent release of the largest leak of classified documents in U.S. military history has turned the Internet into a war zone.

On one side, WikiLeaks has assembled the brightest and most dedicated hacker-activists in an effort to turn the Internet into a bastion of transparency and information freedom.

On the other side, the United States has combined its Department of Defense, Federal Bureau of Investigation, National Security Agency in an attempt to clamp down on the Internet with censorship and encryption-banning laws.

Both parties, however, have fully realized the importance of the Internet and the outcome of their battle will change the face of the world.

The Brimming of a Binary Battle

Earlier this year, WikiLeaks, then only a marginally popular organization, released "Collateral Murder," a YouTube video depicting U.S. soldiers in Iraq murdering civilians, two Reuters journalists and two children.

"Come on, lets shoot," cries Crazyhorse One-Eight, the soldier manning the helicopter machine-gun during the video. "Come on!"

"Oh yeah, look at those dead bastards."

"A lot of my friends are in that video," said Iraq War veteran Josh Stieber to AntiWar Radio. "I would definitely say that that is, nine times out of 10, the way things ended up. Killing was following military protocol. If these videos shock and revolt you, they show the reality of what war is like."

Before the release of the video, the U.S. military repeatedly claimed that the gunfight occurred under its Rules of Engagement and withheld information about the incident from Reuters.

The video caused international outrage. WikiLeaks bloomed into what the U.S. government began to perceive as a dangerous enemy. The world furiously demanded answers while the Federal Bureau of Investigation began an exhaustive search for the whistleblower.

In May, the FBI finally arrested Private First Class Bradley Manning, a 23-year-old American soldier, under suspicion of leaking classified documents.

Manning was betrayed hours earlier by famed hacker-turned-narc Adrian Lamo, who turned over chat logs with Manning to Army Intelligence. Lamo stated that his actions were due to a "crisis of conscience."

According to Lamo, Manning had admitted to leaking more than 260,000 classified diplomatic

cables. WikiLeaks has repeatedly denied receiving such a leak.

At the Hackers On Planet Earth conference in July 2010—a symposium of hackers that discuss the ethics and politics of the Internet—the hacker community mobilized in opposition against Lamo, going as far as having a guest speaker call him a "crazy narc fuck" right after Lamo's talk.

Some state that Lamo's betrayal of Manning may have been an attempt to lessen his own criminal status, including a $60,000 fine for hacking into established companies such as The New York Times and Microsoft. Others blamed his infamous love for press attention.

Manning was imprisoned without parole for weeks in Kuwait, and was later transferred to a military base in Quantico, Virginia, where he is still detained. He is facing a possible half-century prison sentence.

In late June, WikiLeaks founder and Editor-in-Chief Julian Assange reported that he had assigned three civil defence lawyers for Manning, all of which had been refused access to him.

Today, protests are held regularly around the world, hailing Manning as a hero and clamoring for his release. Many dub him as a modern day Daniel Ellsberg, including Ellsberg himself. Ellsberg was a U.S. military analyst who leaked top-secret Pentagon documents about the Vietnam war to a New York Times reporter in 1969.

WikiLeaks was also represented at the conference by Jacob Appelbaum, a well-known computer hacker responsible for breaking Apple's FileVault encryption system as well as managing a large part of Tor, a project that allows almost-perfect anonymity on the web.

"When you ignore the injustices of the world, you are part of the problem," said Appelbaum at the conference, filling in for Assange, who was unable to attend due to his wanted status for leaking classified military information on WikiLeaks. Federal agents were so numerous they were "crawling up the walls," said one source.

"If you've read [about hackers], then you know that you just can't stop us. The purpose here is to give you the data, so that you can make your own analysis," said Appelbaum.

Appelbaum cited distrust of the mainstream media, since its articles never behaved like a scientific journal, whereas WikiLeaks worked on releasing only raw source material free for public interpretation.

"When the media is gagged, we refuse to be gagged," stated Appelbaum. "This whole idea of hunting for [Assange], you can cut off the head—but there will be more."

After his speech, Appelbaum had to use a doppelgänger to escape the rush of federal agents onstage, and at a later unrelated talk was harassed by two FBI agents who asked to have a talk with him so that they could flesh things out.

According to an article on CNet News, an attorney present in the room asked them if they were attending the conference for business or pleasure.

"A little of both," one of them replied.

The Internet had already taken the role of a battleground.

Weeks after the WikiLeaks conference, the site released a cache of over 92,000 classified Afghanistan war documents, free for the world to browse through, conveniently coupling the release with a leaked Central Intelligence Agency document that examines the possibility of the U.S. being perceived as an exporter of terrorism.

The Pentagon, already on a full-swing manhunt for Assange, intensified its war against WikiLeaks. Pentagon spokesmen called for the "return" of the leaked documents—a move that is necessary by law for the Pentagon to be capable of later accusing WikiLeaks of espionage.

The FBI and the U.S. government joined forces, declaring its $9-million "Going Dark" program combined with an Obama-backed bill that would outlaw all encryption that the government can't obtain backdoor access to, thus outlawing all encryption WikiLeaks depends on to provide security for its sources. The U.S. Government aimed to garner an "Eye of Sauron" of the Internet.

In late September, the U.S. government furthered its war against WikiLeaks with a new bill—the Combating Online Infringement and Counterfeits Act—which seems like an anti-piracy bill, if one doesn't bother to closely examine the fine print.

"The list is for domains 'dedicated to infringing activity', which is defined very broadly," said Aaron Swartz on his anti-web-censorship site DemandProgress.org. "Any site where counterfeit goods or copyrighted material are 'central to the activity of the Internet site' would be blocked."

It doesn't seem far-removed for a government that already plans to accuse WikiLeaks of espionage to accuse it of harboring "counterfeit goods." The United States has launched a full-scale attack on the rights, privacy and freedom of its own people in a desperate, scrambling attempt to deal with WikiLeaks's truth-speaking.

An Ideal Held at Gunpoint

In March, WikiLeaks published a classified CIA document that discussed in detail various means the U.S. government could employ to destroy WikiLeaks.

"Websites such as WikiLeaks.org have trust as their most important centre of gravity by protecting the anonymity and identity of the insider, leaker, or whistleblower," the report stated. "Successful identification, prosecution, termination of employment, and exposure of persons leaking the information by the governments and businesses affected by information posted to WikiLeaks.org would damage and potentially destroy this centre of gravity and deter others from taking similar actions."

Many have realized the chilling similarity between the report's suggested strategy for dismantling WikiLeaks and Manning's recent arrest.

"It looks like we're about to be attacked by everything the U.S has," said WikiLeaks via Twitter in June. Those words were prophetic.

Uniting towards their ideal, the world's most talented hackers have gravitated towards WikiLeaks and what it represents, forming the largest political hacktivist group in history. The U.S. found itself facing an enemy it had never prepared for.

The Internet has become a nation, a state, a perfect meritocracy—one that is currently in a state of war.

It has its culture—those who entertain, those who are heroes, those who produce media, those who report, those who play, those who work. It has built a net of mental inhabitants and it has become the first metropolis of its kind, of which a past example is inconceivable. That lack of a prior example is what makes the real world so wary of it.

By architecture, the design of the Internet is fundamentally different from the design of the real world. There cannot possibly be rulers, or any figure of authority in a world of information, but there can be power.

In the meritocracy of the Internet, the capable, astute, intelligent can rise to a position of fame or fortune. Ever since the early days of the Internet, that elite group has been comprised of hackers, because hackers gain knowledge through the usage of systems—meaning power through the inner workings of the Internet.

They rise over the Internet with knowledge of how their environment is built, and the skill to bend it to their own ends.

Thus did Appelbaum work on the Tor project, summoning out of the Internet's architectural infinity a way for anonymous web access. Assange changed the face of classified political information with his ability to will the Internet's design into releasing, into the real world, tens of thousands of secret truths.

The Hackers On Planet Earth conference—where both fallen heroes such as Adrian Lamo and digital superpowers such as WikiLeaks presented talks—was a conference of national power figures meeting to discuss the future of their country.

Their homeland, where they built and were built, had entered a state of war with another nation whose realm of existence was completely different—and in ways superior thanks to its dominance on physical reality.

The U.S. has recently been feeling attacked by the Internet in the only way the Internet could ever wage a war: with information. In a leaderless universe, Assange, a hacker himself in his earlier years, achieved what catapulted him into a position of dominance and respect in his homeland, and controversy and revulsion in the country he concerns himself with.

Unlike the Internet, the U.S. has rulers, and those rulers aren't yet accustomed to how the people of the Internet see knowledge as free. In fact, they are threatened by it.

The behaviour of both parties concerned with this issue has indicated that they are currently in a state of war. The U.S. government attempts to antagonize the enemy, arouse public hatred and fear of it, uproot it, dissolve it, and even give its leaders the kill switch to completely annihilate all presence of the Internet from its country.

The United States seeks to use its dominance of space as an advantage over the Internet. The Internet, on the other hand, is seeking to use a complete opposite: the lack of space, the lack of time, in order to have complete control over what matters: information.

As WikiLeaks releases more information, they have received more threats from the U.S. governement. The U.S is responding to a war that it, in its opinion, did not initiate—WikiLeaks sees itself as on a mission to provide to the entire Internet the truth about the real world, in a spirit of justice. Those concerned in the real world see their constructs as being threatened by an

independent, self-sufficient third party no one had ever imagined.

The resulting aggression we see today is a sign of a shock at the dimensions of the fight. No nation has ever fought, or even imagined, a war with a nation that has no homeland and a people with no identity. And thus does the U.S finds both its rulers and its laws punishing the truth-speaking and fighting those who stick by their own motto of truth and bravery.

The only way this war will end is if both sides realize that this is the closest we have come to a war-of-the-worlds: the Internet and the real world are that far apart. This is a battle of applied ethics: information transparency versus the ideal that some are more fit to know than others.

There is no question that the side that will win this ethical battle will be the one to define, at least for the coming decade, if information transparency is nurturing or destructive.

Nadim Kobeissi is a computer network security analyst based in Montreal.

http://thelinknewspaper.ca/article/517
