US officials announce formation of offensive cyber war units

Alex Lantier
14 March 2013

In testimony before US Senate committees, top US intelligence officials announced Tuesday that Washington is setting up military units to wage offensive cyber war—i.e., to write malicious computer code to disable or destroy computers and computer-controlled infrastructure.

These statements came as US officials escalated their denunciations of China, which they allege is engaged in cyber-espionage of US firms. On Monday, US National Security Advisor Tom Donilon demanded that China investigate alleged attacks "emanating from China on an unprecedented scale," and agree to broad negotiations on protocols for Internet use.

General Keith Alexander, the head of the National Security Agency (NSA) and commander of the US Cyber Command, told the Senate Committee on Armed Services: "I would like to be clear that this team, this defend-the-nation team, is not a defensive team. This is an offensive team that the Defense Department would use to defend the nation if it were attacked in cyberspace. Thirteen of the teams that we are creating are for that mission alone."

According to Alexander, there are 13 US offensive cyber war teams, interacting with 27 other cyber war teams deployed with standard military commands. The offensive teams are overseen by the US Cyber Command, which operates on the premises of the NSA and has a budget of $191 million this year.

The importance of cyber-warfare has grown with the increasing use of computers to control key infrastructure. A sophisticated cyber-attack could potentially take down or destroy power plants, hospitals, transport systems and other critical infrastructure. While this provocative US military escalation is supposedly driven by the risk of a devastating cyber-attack from China or other countries, US intelligence officials acknowledge that the risk of such an attack is very small.

Testifying before the Senate Intelligence Committee, US Director of National Intelligence James Clapper said there was only a "remote chance" of a serious attack, which he defined as one leading to "long-term, wide-scale disruption of services, such as a regional power outage."

Clapper's prepared statement listed China and Russia as "advanced cyber actors" with the capacity to mount such an attack. However, he added, they "are unlikely to launch such a devastating attack against the United States outside of a military conflict or crisis that they believe threatens their vital interests."

Nonetheless, Clapper claimed that such an attack was the most serious immediate threat to the US, outweighing the threat of attacks by terrorist groups such as Al Qaeda.

General Alexander's prepared statement to the armed services committee suggested that the US Cyber Command's main concern is not so much the risk of a devastating attack from abroad, but the risk to US corporations' profit interests.

Decrying what he called the "greatest unwilling transfer of wealth in history," Alexander wrote: "We have some confidence in our ability to deter major state-on-state attacks in cyberspace, but we are not deterring the seemingly low-level harassment of private and public sites, property, and data… The damage they are doing to America's economic competitiveness and innovation edge is profound, translating into missed opportunities for US companies and the potential for lost American jobs. Cyber-enabled theft jeopardizes our economic growth."

The cyber war escalation announced by Alexander and Clapper is provocative and reckless. The US

military is engaging in essentially criminal activity—writing computer viruses—while acknowledging that it is unlikely that the United States will face such an attack. The Pentagon aims not to deter or defend against an attack, but to provide further means for aggression and intimidation against any power Washington considers to be a significant geo-strategic obstacle or economic rival.

The official justification for this escalation, based on unsubstantiated assertions that hackers in China are being sponsored by the Chinese government and military in an effort to harm the United States, falsely paints the United States government as being as on the defensive.

In fact, Washington is the world's most ruthless practitioner of cyber warfare. Working with Israel, it used the Stuxnet virus to disrupt Iran's nuclear program by manipulating and destroying centrifuges at the Natanz plant. The US designed the Flame virus to spy on Iranian officials. The Flame virus itself was discovered last year, after it escaped from Iranian government networks and began infecting computers in the general population.

US officials openly discuss cyber warfare as a weapon in the Pacific, where Washington is now mounting a "pivot to Asia" aimed at China. On Monday, the American Forces Press Service (AFPS) discussed cyber war with Brigadier General John Hicks, the commander of the Pacific Fleet's cyber war unit, which reportedly served as a "test bed" for the US Cyber Command.

Describing Pacific Fleet exercises involving simulated cyber-attacks on naval communications, Hicks said: "The intent is to be a fusion center to integrate cyber in all its versions in the entire cyber portfolio into the command's daily and war-fighting battle rhythm… Nothing happens out here, we don't have visibility on anything, we can't command and control anything, my boss Admiral [Samuel] Locklear can't do his mission without assured and secure communications."

The AFPS commented, "The cyber domain is the new military 'high ground'—an advantage to those who use it effectively, and the downfall of those who don't."

Like the German Empire's decision to wage unrestricted submarine warfare nearly one century ago, during World War I, this expansion of the methods of war is sinister and belligerent. While cyber-attacks have the potential to cause immense damage, it is also easy for hackers to disguise their identity while launching them by taking over other people's computers and disseminating code from there. As US attacks on Iran have already shown, this opens a wide field for provocations and false-flag attacks.

Nonetheless, Washington is plowing immense resources into cyber war, feeding a global arms race to design the most destructive computer viruses. The US government has already claimed the right to launch pre-emptive cyber strikes if the president orders them, even if the US is not at war with the targeted country. (See: "Obama administration claims power to authorize pre-emptive cyber-war strikes")

Though US cyber war plans target China, Iran and other countries, they are also directed against the democratic rights of the American people.

Alexander testified that defense against cyber-attack depended on real-time monitoring of incoming Internet traffic to the United States by private Internet Service Providers, which would give all necessary information to US authorities. This amounts to a blank check for unlimited, real-time Internet spying by the US government on the American people and anyone with whom they are communicating abroad.

Alexander testified that his officers already work closely with US domestic security services and unnamed private firms. In his written testimony, he explained: "We at USCYBERCOM are also helping DoD [the Department of Defense] increase our global situational awareness through our growing collaboration with federal government mission partners like the Department of Homeland Security (DHS), the FBI, and other departments and agencies, as well as with private industry and with other countries."