Obama orders US to draw up overseas target list for cyber-attacks

Exclusive: Top-secret directive steps up offensive cyber capabilities to 'advance US objectives around the world'

• Read the secret presidential directive here

Glenn Greenwald and **Ewen MacAskill**
theguardian.com, Friday 7 June 2013 20.06 BST

Jump to comments (…)

Link to video: Obama defends internet surveillance programs

Barack Obama has ordered his senior national security and intelligence officials to draw up a list of potential overseas targets for US cyber-attacks, a top secret presidential directive obtained by the Guardian reveals.

The 18-page Presidential Policy Directive 20, issued in October last year but never published, states that what it calls Offensive Cyber Effects Operations (OCEO) "can offer unique and unconventional capabilities to advance US national objectives around the world with little or no warning to the adversary or target and with potential effects ranging from subtle to severely damaging".

It says the government will "identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power".

Article history

The NSA Files: Decoded

What the surveillance revelations mean for you

World news
US national security · Barack Obama · United States · US foreign policy · China · Privacy · The NSA files

Technology
Cybercrime · Hacking · Data protection

Series
Glenn Greenwald on security and liberty

More from Glenn Greenwald on security and liberty on

World news
US national security · Barack Obama · United States · US foreign policy · China · Privacy · The NSA files

Technology
Cybercrime · Hacking · Data protection

More news

The directive also contemplates the possible use of cyber actions inside the US, though it specifies that no such domestic operations can be conducted without the prior order of the president, except in cases of emergency.

The aim of the document was "to put in place tools and a framework to enable government to make decisions" on cyber actions, a senior administration official told the Guardian.

The administration published some declassified talking points from the directive in January 2013, but those did not mention the stepping up of America's offensive capability and the drawing up of a target list.

Obama's move to establish a potentially aggressive cyber warfare doctrine will heighten fears over the increasing militarization of the internet.

The directive's publication comes as the president plans to confront his Chinese counterpart Xi Jinping at a summit in California on Friday over alleged Chinese attacks on western targets.

Even before the publication of the directive, Beijing had hit back against US criticism, with a senior official claiming to have "mountains of data" on American cyber-attacks he claimed were every bit as serious as those China was accused of having carried out against the US.

Presidential Policy Directive 20 defines OCEO as "operations and related programs or activities … conducted by or on behalf of the United States Government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States government networks."

Asked about the stepping up of US offensive capabilities outlined in the directive, a senior administration official said: "Once humans develop the capacity to build boats, we build navies. Once you build airplanes, we build air forces."

The official added: "As a citizen, you expect your government to plan for scenarios. We're very interested in having a discussion with our international partners about what the appropriate boundaries are."

The document includes caveats and precautions stating that all US cyber operations should conform to US and international law, and that any operations "reasonably likely to result in significant consequences require specific presidential approval".

The document says that agencies should consider the consequences of any cyber-action. They include the impact on intelligence-gathering; the risk of retaliation; the impact on the stability and security of the internet itself; the balance of political risks versus gains; and the establishment of unwelcome norms of international behaviour.

Among the possible "significant consequences" are loss of life; responsive actions against the US; damage to property; serious adverse foreign policy or economic impacts.

The US is understood to have already participated in at least one major cyber attack, the use of the Stuxnet computer worm targeted on Iranian uranium enrichment centrifuges, the legality of which has been the subject of controversy. US reports citing high-level sources within the intelligence services said the US and Israel were responsible for the worm.

In the presidential directive, the criteria for offensive cyber operations in the directive is not limited to retaliatory action but vaguely framed as advancing "US national objectives around the world".

The revelation that the US is preparing a specific target list for offensive cyber-action is likely to reignite previously raised concerns of security researchers and academics, several of whom have warned that large-scale cyber operations could easily escalate into full-scale military conflict.

Sean Lawson, assistant professor in the department of communication at the University of Utah, argues: "When militarist cyber rhetoric results

More on this story

US intelligence outlines checks it says validate surveillance
Intelligence chiefs confirm programmes, but say they protect against terrorism and minimise infringements on privacy

Edward Snowden is a 'traitor' and possible spy for China – Dick Cheney

Do not extradite Edward Snowden, protesters urge Hong Kong

Edward Snowden supporters march in Hong Kong – in pictures

Snowden gains support from protesters - video

Facebook, Microsoft reveal surveillance request figures

John Naughton: A boycott of Facebook, Microsoft, Google et al almost impossible to achieve

Guardian poll finds majority in US want greater oversight

Prism surveillance 'did not collect European data in bulk'

Edward Snowden story on way to the big screen

NSA to release details of attacks it claims were foiled by surveillance

Welcome to Utah, the NSA's desert home for eavesdropping on America

A Guardian guide to metadata

The story of the scoop

What we know about Snowden

Snowden's girlfriend: At the moment I feel alone

Google asks DoJ for permission to publish Fisa requests

Video

Ford dances to Bob Marley's One Love

From Danwei.com

Police bust PR companies for illegal deletion of news and social media postings

Hybrid cars: BYD's new Qin

in use of offensive cyber attack it is likely that those attacks will escalate into physical, kinetic uses of force."

An intelligence source with extensive knowledge of the National Security Agency's systems told the Guardian the US complaints again China were hypocritical, because America had participated in offensive cyber operations and widespread hacking – breaking into foreign computer systems to mine information.

Provided anonymity to speak critically about classified practices, the source said: "We hack everyone everywhere. We like to make a distinction between us and the others. But we are in almost every country in the world."

The US likes to haul China before the international court of public opinion for "doing what we do every day", the source added.

One of the unclassified points released by the administration in January stated: "It is our policy that we shall undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as preferred courses of action."

The full classified directive repeatedly emphasizes that all cyber-operations must be conducted in accordance with US law and only as a complement to diplomatic and military options. But it also makes clear how both offensive and defensive cyber operations are central to US strategy.

Under the heading "Policy Reviews and Preparation", a section marked "TS/NF" - top secret/no foreign - states: "The secretary of defense, the DNI [Director of National Intelligence], and the director of the CIA … shall prepare for approval by the president through the National Security Advisor a plan that identifies potential systems, processes and infrastructure against which the United States should establish and maintain OCEO capabilities…" The deadline for the plan is six months after the approval of the directive.

The directive provides that any cyber-operations "intended or likely to produce cyber effects within the United States" require the approval of the president, except in the case of an "emergency cyber action". When such an emergency arises, several departments, including the department of defense, are authorized to conduct such domestic operations without presidential approval.

Obama further authorized the use of offensive cyber attacks in foreign nations without their government's consent whenever "US national interests and equities" require such nonconsensual attacks. It expressly reserves the right to use cyber tactics as part of what it calls "anticipatory action taken against imminent threats".

The directive makes multiple references to the use of offensive cyber attacks by the US military. It states several times that cyber operations are to be used only in conjunction with other national tools and within the confines of law.

When the directive was first reported, lawyers with the Electronic Privacy Information Center filed a Freedom of Information Act request for it to be made public. The NSA, in a statement, refused to disclose the directive on the ground that it was classified.

In January, the Pentagon announced a major expansion of its Cyber Command Unit, under the command of General Keith Alexander, who is also the director of the NSA. That unit is responsible for executing both offensive and defensive cyber operations.

Earlier this year, the Pentagon publicly accused China for the first time of being behind attacks on the US. The Washington Post reported last month that Chinese hackers had gained access to the Pentagon's most advanced military programs.

The director of national intelligence, James Clapper, identified cyber threats in general as the top national security threat.

Law abiding citizens have 'nothing to fear', says Hague
The foreign secretary, William Hague, says reports that GCHQ are gathering intelligence from phones and online sites should not concern people who have nothing to hide

Obama defends internet surveillance programmes

Comment & analysis

On Prism, partisanship and propaganda
Glenn Greenwald: Addressing many of the issues arising from last week's NSA stories

Glenn Greenwald: Edward Snowden's worst fear has not been realised – thankfully

Investigate Booz Allen Hamilton, not Edward Snowden

Julian Borger: How Edward Snowden weakened the case for his defence

Ai Weiwei: US is behaving like China

Glenn Greenwald: on whistleblowers and government threats of investigation

Internet Poll on changing China's strange public holiday system

A Brief Guide to China's Media Landscape

Li Xiaolai, Bitcoin millionaire

More from Danwei

On World news

Most viewed | Latest

Last 24 hours

1. Robin Thicke named sexist of the year
2. New York City puts e-cigarettes under smoking ban
3. Obama commutes sentences of eight crack cocaine offenders
4. Mikhail Khodorkovsky freed after pardon from Vladimir Putin
5. Vladimir Putin pardons jailed oil tycoon Mikhail Khodorkovsky

More most viewed

Last 24 hours

1. Eyewitness: Edinburgh
2. Mikhail Khodorkovsky freed after pardon from Vladimir Putin
3. South Sudan stands at precipice, says Barack Obama
4. Toyota: Abbott uninterested in providing asssistance, says union
5. Fatal asylum seeker sinkings: agencies urged to improve rescue co-ordination

All today's stories

guardianbookshop

This week's bestsellers

1. **Stoner**
by John L Williams
£7.19
2. **Stephen Ward Was Innocent, OK**
by Geoffrey Robertson £9.74
3. **Guardian Quick Crosswords 5 & 6**
£8.00
4. **Tales from the Secret Footballer**
£7.99
5. **Ammonites and Leaping Fish**
by Penelope Lively £10.99

Obama officials have repeatedly cited the threat of cyber-attacks to advocate new legislation that would vest the US government with greater powers to monitor and control the internet as a means of guarding against such threats.

One such bill currently pending in Congress, the Cyber Intelligence Sharing and Protection Act (Cispa), has prompted serious concerns from privacy groups, who say that it would further erode online privacy while doing little to enhance cyber security.

In a statement, Caitlin Hayden, national security council spokeswoman, said: "We have not seen the document the Guardian has obtained, as they did not share it with us. However, as we have already publicly acknowledged, last year the president signed a classified presidential directive relating to cyber operations, updating a similar directive dating back to 2004. This step is part of the administration's focus on cybersecurity as a top priority. The cyber threat has evolved, and we have new experiences to take into account.

"This directive establishes principles and processes for the use of cyber operations so that cyber tools are integrated with the full array of national security tools we have at our disposal. It provides a whole-of-government approach consistent with the values that we promote domestically and internationally as we have previously articulated in the International Strategy for Cyberspace.

"This directive will establish principles and processes that can enable more effective planning, development, and use of our capabilities. It enables us to be flexible, while also exercising restraint in dealing with the threats we face. It continues to be our policy that we shall undertake the least action necessary to mitigate threats and that we will prioritize network defense and law enforcement as the preferred courses of action. The procedures outlined in this directive are consistent with the US Constitution, including the president's role as commander in chief, and other applicable law and policies."

Comments

More from Glenn Greenwald on security and liberty

A critical, campaigning column on vital issues of civil rights, freedom of information and justice – and their enemies, from the award-winning journalist, former constitutional litigator and author of three New York Times bestsellers.

Follow @ggreenwald on Twitter or email him at glenn.greenwald@guardiannews.com

Latest:
31 Oct 2013: On leaving the Guardian | Glenn Greenwald

Next:
7 Jun 2013: NSA Prism program taps in to user data of Apple, Google and others

Previous:
7 Jun 2013: On whistleblowers and government threats of investigation | Glenn Greenwald

Glenn Greenwald on security and liberty index