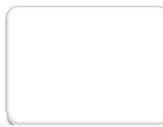


What Works in a Crisis?

This investment beats stocks, gold --Up every year since 1992

(11.100%)



[Home](#) | [Video](#) | [Themen](#) | [Forum](#) | [English](#) | **DER SPIEGEL** | **SPIEGEL TV** | [Abo](#) | [Shop](#)

SPIEGEL ONLINE INTERNATIONAL

[Front Page](#) [World](#) [Europe](#) [Germany](#) [Business](#) [Zeitgeist](#) [Newsletter](#)

[English Site](#) > [World](#) > [NSA Spying Scandal](#) > New Snowden Docs Indicate Scope of NSA Preparations for Cyber Battle

The Digital Arms Race: NSA Preps America for Future Ba

By Jacob Appelbaum, Aaron Gibson, Claudio Guarnieri, Andy Müller-Maguhn, Laura Poitras, Marc Schneier, Hilmar Schmundt and Michael Sontheimer



The NSA's mass surveillance is just the beginning. Documents from Edward Snowden show that the intelligence agency is arming America for future digital wars -- a struggle for control of cyberspace is already well underway.

January 17, 2015 – 05:07 PM

Share

Recommend

203

Tweet

599

8

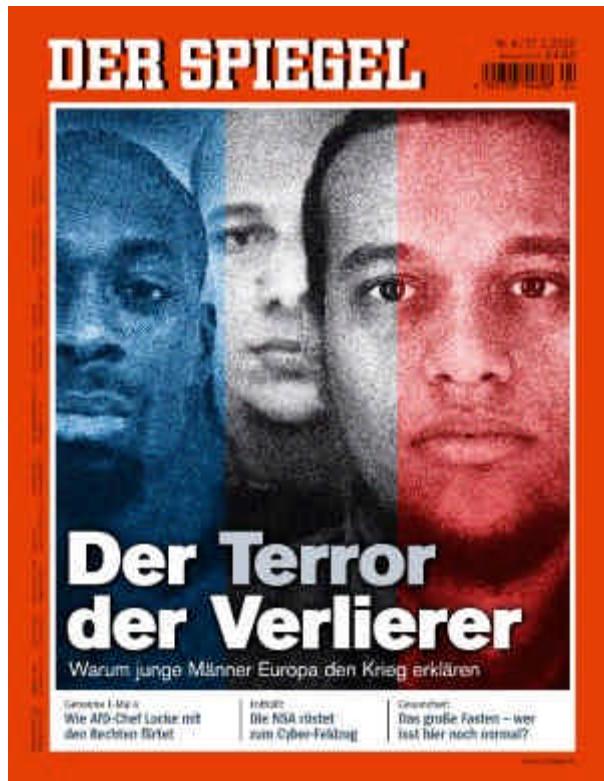
[Print](#) | [E-Mail](#)

[Feedback](#)

Normally, internship applicants need to have political connections or volunteer work on social projects considered a plus. But the job posting calls for candidates with significantly more experience.

Comment

From DER SPIEGEL



The article you are reading originally appeared in German in issue 4/2015 (January 17, 2015) of DER SPIEGEL.

Click on the links below for more information about DER SPIEGEL's history, how to subscribe or purchase the latest issue of the German-language edition in print or digital form or how to obtain rights to reprint SPIEGEL articles.

Frequently Asked Questions: Everything You Need to Know about DER SPIEGEL

Six Decades of Quality Journalism: The History of DER SPIEGEL

A New Home in HafenCity: SPIEGEL's New Hamburg HQ

Reprints: How To License SPIEGEL Articles

NSA Spying Scandal

National Security Agency

Government Communications Headquarters

Data Protection

are, the ad says, "looking for interns who want to

Politerain is not a project associated with a conventional company. It is run by a US government intelligence organization, the National Security Agency (NSA). More precisely, it's operated by the NSA's digital snipers with Tailored Access Operations (TAO), the department responsible for breaking into computers.

Potential interns are also told that research into third party computers might include plans to "remotely degrade or destroy op routers, servers and network enabled devices by hardware." Using a program called Passionatepol may be asked to "remotely brick network cards." Berserk they would implant "persistent backdoor drivers". Using another piece of software called B "erase the BIOS on a brand of servers that act as rival governments."

An intern's tasks might also include remotely des of hard drives. Ultimately, the goal of the internst "developing an attacker's mindset."

The internship listing is eight years old, but the a since become a kind of doctrine for the NSA's dat intelligence service isn't just trying to achieve m Internet communication, either. The digital spies -- comprised of the United States, Britain, Canad Zealand -- want more.

The Birth of D Weapons

According to top secret documents from the archi Edward Snowden seen exclusively by SPIEGEL, th wars of the future in which the Internet will play a aim of being able to use the net to paralyze comp doing so, potentially all the infrastructure they co and water supplies, factories, airports or the flow

During the 20th century, scientists developed so- atomic, biological and chemical. It took decades l could be regulated and, at least partly, outlawed.

Photo Gallery



Photo Gallery: What the Intelligence Agencies Can and Cannot Do

SPIEGEL's Top NSA Reports



DPA/ NSA

Prying Eyes: Inside the NSA's War on Internet Security

Obama's Lists: A Dubious History of Targeted Killings in Afghanistan

Spying Together: Germany's Deep Cooperation with the NSA

The NSA in Germany: Snowden's Documents Available for Download

New NSA Revelations: Inside Snowden's Germany File

'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel

NSA's Secret Toolbox: Unit Offers Spy Gadgets for Every Need

Inside TAO: Documents Reveal Top NSA Hacking Unit

Friendly Fire: How GCHQ Monitors Germany, Israel and the EU

Embassy Espionage: The NSA's Secret Spy Hub in Berlin

iSpy: How the NSA Accesses Smartphone Data

Codename 'Apalachee': How America Spies on Europe and the UN

Cover Story: How the NSA Targets Germany and Europe

have now been developed for the war on the Internet. There are almost no international conventions or supervisor weapons, and the only law that applies is the surveillance law.

Canadian media theorist Marshall McLuhan foresaw this decades ago. In 1970, he wrote, "World War III is not a war with no division between military and civilian. It is precisely the reality that spies are preparing for today."

The US Army, Navy, Marines and Air Force have their own cyber forces, but it is the NSA, also officially known as the National Security Agency, that is taking the lead. It's no coincidence that the director of the NSA also serves as the head of the US Cyber Command. The data spy, Admiral Michael Rogers, is also its chief. Close to 40,000 employees are responsible for both offensive and defensive destructive network attacks.

Surveillance only 'Phase 0'

From a military perspective, surveillance of the Internet is the first step in the US digital war strategy. Internal NSA documents show that surveillance is the prerequisite for everything that follows. The goal of the surveillance is to detect vulnerabilities in enemy networks. "Stealthy implants" have been placed to infiltrate them, allowing "permanent accesses," then Phase Three, a phase headed by the word "dominate" in the documents, allows them to "control/destroy critical systems & networks." Pre-positioned accesses (laid in Phase 0). Critical infrastructure is considered by the agency to be anything that is important to society running: energy, communications and transportation. Documents state that the ultimate goal is "real time escalation".

One NSA presentation proclaims that "the next war will be fought in cyberspace." To that end, the US government is conducting a massive effort to digitally arm itself for network warfare. In the secret intelligence budget, the NSA projected it would spend \$1 billion in order to increase the strength of its communication operations. The budget included an increase of so-called "unconventional solutions" alone.

NSA Docs on Network Attacks and Exploits

Excerpt from the secret NSA budget on computer network attacks: The budget includes a new word **GENIE**.

Document about the expansion of the Remote Operations Center (ROC) endpoint operations:

Document explaining the role of the Remote Operations Center (ROC):

Related SPIEGEL ONLINE links

Prying Eyes: Inside the NSA's War on Internet Security (12/28/2014)

NSA Documents: Attacks on VPN, SSL, TLS, SSH, Tor (12/28/2014)

Obama's Lists: A Dubious History of Targeted Killings in Afghanistan (12/28/2014)

Inside TAO: Documents Reveal Top NSA Hacking Unit (12/29/2013)

Get Mobile with Our New App



Download It Today: 'DER SPIEGEL in English' Now Available for iPhone

European Partners

 Presseurop

 Politiken

 Corriere della Sera

Municipalities' Spending Madness

20 Rome Jihadists Investigated

Newsletter



Sign up for Spiegel Online's daily newsletter - and get **the best** of Der Spiegel's and Spiegel Online's international coverage in your In-Box **everyday**.

Facebook

Interview with an employee of NSA's department for Operations about his field of work

Supply-chain interdiction / Stealthy techniques can hardest targets

Classification guide for computer network exploitation

NSA training course material on computer network

Overview of methods for NSA integrated cyber operations

NSA project description to recognize and process direct and indirect party attacks on computers

Exploring and exploiting leaky mobile apps with BA

Overview of projects of the TAO/ATO department such as destruction of network cards

iPhone target analysis and exploitation with Apple's unique identifiers (UDID)

Report of an NSA Employee about a Backdoor in the

NSA document on QUANTUMSHOOTER, an implant that can infect computers with good network connections from un

In recent years, malware has emerged that experts believe was developed by the NSA and its Five Eyes alliance based on a number of programs. One of these include programs like Stuxnet, used to attack the Iranian nuclear program. Or Regin, a powerful spyware trojan that was discovered in Germany after it infected the USB stick of a high-ranking official, German Chancellor Angela Merkel. Agents also used Regin to spy on the European Commission, the EU's executive, and Belgian telecommunications company Belgacom in 2011.

Given that spies can routinely break through just about any software, virtually all Internet users are at risk of being targeted.

The new documents shed some new light on other NSA projects. Although an attack called Quantuminsert has been mentioned in previous SPIEGEL and others' documentation, it appears to have had a success rate and it has likely been replaced by another program called Quantumdirk, which injects malicious content provided by websites such as Facebook and Yahoo. An iPhone infected with Straitbizarre can be turned into a non-attributable "shooter" node. These nodes can receive messages from the NSA's Quantum network, which provides the command and control for very large scale active exploitation. NSA agents were also able to breach mobile phones' security vulnerability in the Safari browser in order to obtain sensitive information remotely and implant malicious code.

In this guerilla war over data, little differentiation is made between soldiers and civilians, the Snowden documents show.

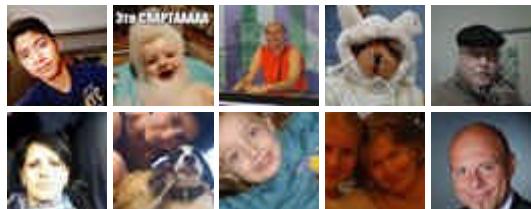
Find us on Facebook



SPIEGEL International

Like

274,828 people like SPIEGEL International.



Facebook social plugin

Twitter



SPIEGEL English

@SPIEGEL_English

3h

SPIEGEL story on #NSA prepping US for Internet battle includes 36 new docs from whistleblower #Snowden's archive. spon.de/aepNt via

Retweeted by Bethany Horne

Show Summary



SPIEGEL English

@SPIEGEL_English

3h

New #Snowden docs cast light on America's digital arms race and how the #NSA is preparing US for war of the future. spon.de/aepNt

Retweeted by Atea #JeSuisAlfon

Show Summary

[Follow @SPIEGEL_English](#)

could suffer damage to his or her data or comput potential to create perils in the offline world as w weapon like Barnfire were to destroy or "brick" th hospital as a result of a programming error, peop mobile phone could be affected.

Intelligence agencies have adopted "plausible de guiding principle for Internet operations. To ensu they seek to make it impossible to trace the auth

It's a stunning approach with which the digital sp undermine the very foundations of the rule of law approach threatens to transform the Internet into superpowers and their secret services operate ac whims with very few ways to hold them accounta

NSA Docs on Malware and Implants

CSEC document about the recognition of trojans and anomaly"

The formalized process through which analysts cho requirement and then get to know the tools that can QUANTUMTHEORY is a set of technologies allowing interference attacks on TCP/IP connections (includ and DAREDEVIL)

Sample code of a malware program from the Five E

Attribution is difficult and requires considerable fo new documents there are at least a few pointers. a keylogger that was part of the Snowden archive software designed to surreptitiously intercept all by the victim and record them for later inspectio indeed rather dated, keylogger. Similar software numerous applications, so it doesn't seem to pos but the sourcecode contained in it does reveal so They suggest that this keylogger might be part of modules that that belong to the Warriorpride prog Esperanto software used by all the Five Eyes part times was even able to break into iPhones, amon documents published by SPIEGEL include sample keylogger to foster further research and enable t appropriate defenses.

'Just a Bunch of Hackers'

The men and women working for the Remote Op which uses the codename S321, at the agency's I Meade, Maryland, work on one of the NSA's most

responsible for covert operations. S321 employee third floor of one of the main buildings on the NSA report from the Snowden archive, an NSA man re when they got started, the ROC people were "just Initially, people worked "in a more ad hoc manner. Nowadays, however, procedures are "more systematic management massively expanded the ROC group. In 2005, the department's motto was, "Your data is equipment is our equipment."

NSA Docs on Exfiltration

[Explanation of the APEX method of combining passive methods to exfiltrate data from networks attacked](#)

[Explanation of APEX shaping to put exfiltrating network patterns that allow plausible deniability](#)

[Presentation on the FASHIONCLEFT protocol that traces and exfiltrate data from trojans and implants to the NSA](#)

[Methods to exfiltrate data even from devices which are offline](#)

[Document detailing SPINALTAP, an NSA project to collect active operations and passive signals intelligence](#)

[Technical description of the FASHIONCLEFT protocol to exfiltrate data from Trojans and implants to the NSA](#)

The agents sit in front of their monitors, working round the clock. Just how close the NSA has already gotten to "network dominance" is illustrated particularly well by the department S31177, codenamed Transgression.

The department's task is to trace foreign cyber attacks, analyze them and, in the best case scenario, to send them to competing intelligence agencies. This form of "Cyber Intelligence" counts among the most delicate forms of

[Part 1: NSA Preps America for Future Battle](#)

[Part 2: How the NSA Reads Over Shoulders of Other Spies](#)

Article...

Pri

Share

Recommend

203 people recommend this what your friends recommend

Tweet 599

g+1 +16 Recommend this



Comments

Discuss this issue with other readers!

Share your opinion!

Share your thoughts

Please register to add a comment.

Subject

optional

Comment

Endpoint Threat Detection

 ziften.com/new-451-research/

New 451 Research -Endpoint Security Get Endpoint Protection Now
Retire On \$1300 Per Month

 liveandinvestoverseas.com

Free Report: The 8 Best Places To Retire In Style Overseas Today

Safe Step® Walk-In Tubs

 safestepubt.com/Free-Estimates

Bathe Safely And Easily Again! BBB Member. Includes Install & Wa
Is He Cheating On You?

 spokeo.com/Cheating-Spouse-Search

Enter His Email Address. See Hard To Find Pics & Social Profiles N
Want to Live in Colombia?

 internationalliving.com

Free report for people considering Visiting or Living in Colombia

Cheap Airline Tickets

 cheapoair.com/Call@1-888-516-7925

Get Direct Deals on 450+ Airlines with CheapOair®. Book Now & S

Concealed Carry Guide

 usconcealedcarry.net

Do You Know Your Rights? Get Your Free Concealed Carry Guide

Usd Canadian Dollar

 wallstreetdaily.com/Top-Currencies

Power Shift In The Currency Market. 3 Currencies Set To Rise By

Keep track of the news

Stay informed with our free news services:

All news from SPIEGEL International

All news from World section

MORE FROM SPIEGEL INTERNATIONAL

GERMAN POLITICS



Merkel's Moves: Power Struggles in Berlin

WORLD WAR II



Truth and Reconciliation: Why the War Still Haunts Europe

ENERGY



Green Power: The Future of Energy

EUROPEAN UNION



United Europe: A Continental Project

OVERVIEW

[Home](#) [Politik](#) [Wirtschaft](#) [Panorama](#) [Sport](#) [Kultur](#) [Netzwerk](#) [Wissenschaft](#) [Gesundheit](#) [einestages](#) [Uni](#) [Reise](#)

DIENSTE

Schlagzeilen
Nachrichtenarchiv
RSS
Newsletter
Mobil

VIDEO

Nachrichten Videos
SPIEGEL TV Magazin
SPIEGEL TV Programm
SPIEGEL Geschichte
SPIEGEL TV Wissen

MEDIA

SPIEGEL QC
Mediadaten
Selbstbuchungstool
weitere Zeitschriften

MAGAZINE

DER SPIEGEL
Dein SPIEGEL
SPIEGEL GESCHICHTE
SPIEGEL WISSEN
KulturSPIEGEL
UniSPIEGEL

SPIEGEL GRUPPE

Abo
Shop
SPIEGEL TV
manager magazin
Harvard Business Ma
buchreport
buch aktuell
Der Audio Verlag
SPIEGEL-Gruppe