

# What Works in a Crisis?

This investment beats stocks, gold --Up every year since 1992  
(4,100%)



[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 Battle

By [Jacob Appelbaum](#), [Aaron Gibson](#), [Claudio Guarnieri](#), [Andy Müller-Maguhn](#), [Laura Poitras](#), [Marco Hilmar Schmundt](#) and [Michael Sontheimer](#)



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

January 17, 2015 – 05:07 PM

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

[Feedback](#)

**Share**

**Recommend** 203

**Tweet** 599



Normally, internship applicants need to have political volunteer work on social projects considered a plus. A job posting calls for candidates with significantly

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." Berserkr 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 ma Internet communication, either. The digital spies -- comprised of the United States, Britain, Canada 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

---

## Related SPIEGEL ONLINE links

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

Canadian media theorist Marshall McLuhan foresaw this reality decades ago. In 1970, he wrote, "World War III is not a war with no division between military and civilian, but 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, which is taking the lead. It's no coincidence that the director of the NSA, Admiral Michael Rogers, also serves as the head of the US Cyber Command. The NSA's data spy, Admiral Michael Rogers, is also its chief. The NSA has close to 40,000 employees are responsible for both defensive and destructive network attacks.

### Surveillance only 'Phase 0'

From a military perspective, surveillance of the Internet is the "Phase 0" in the US digital war strategy. Internal NSA documents state 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 enemy networks, allowing "permanent accesses," then Phase Three begins: a phase headed by the word "dominate" in the documents. The goal is to "control/destroy critical systems & networks." The NSA has pre-positioned accesses (laid in Phase 0)." Critics consider this considered by the agency to be anything that is in the public interest: society running: energy, communications and transportation. Documents state that the ultimate goal is "real time escalation".

One NSA presentation proclaims that "the next battle will be 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 \$1.5 billion in order to increase the strength of its cyber operations. The budget included an increase of \$500 million for "unconventional solutions" alone.

---

## NSA Docs on Network Attacks and Exploitation

**Excerpt from the secret NSA budget on computer network operations word GENIE**

**Document about the expansion of the Remote Operations and endpoint operations**

**Document explaining the role of the Remote Operations and endpoint operations**

**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)

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

**Supply-chain interdiction / Stealthy techniques can hit hardest targets**

**Classification guide for computer network exploitation**

**NSA training course material on computer network exploitation**

**Overview of methods for NSA integrated cyber operations**

**NSA project description to recognize and process data from party attacks on computers**

**Exploring and exploiting leaky mobile apps with Backdoor**

**Overview of projects of the TAO/ATO department's destruction of network cards**

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

**Report of an NSA Employee about a Backdoor in the NSA document on QUANTUMSHOOTER, an implant that targets computers with good network connections from untrusted sources**

## 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



SPIEGEL ONLINE

**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

In recent years, malware has emerged that exploits the NSA and its Five Eyes alliance based on a number of 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 German official. Agents also used Regin to infiltrate the European Commission, the EU's executive, and Belgian 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 malware. Although an attack called [Quantuminsert](#) has been reported in SPIEGEL and others, documentation shows that its success rate and it has likely been replaced by malware as Quantumdirk, which injects malicious content into websites provided by websites such as Facebook and Yahoo. Malware infected with Straitbizarre can be turned into disposable non-attributable "shooter" nodes. These nodes can intercept messages from the NSA's Quantum network, which provides access and control for very large scale active exploitation. Secret agents were also able to breach mobile phone vulnerabilities in the Safari browser in order to obtain and remotely implant malicious code.

In this guerilla war over data, little differentiators between soldiers and civilians, the Snowden documents show that the NSA is targeting everyone.

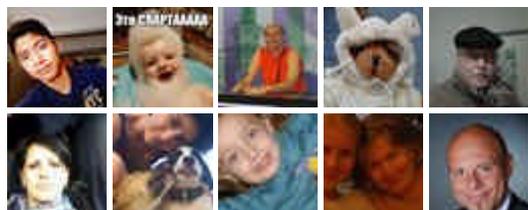
Find us on Facebook



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](http://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](http://spon.de/aepNt)

Retweeted by Atea #JeSuisAlfon

Show Summary

Follow @SPIEGEL\_English

could suffer damage to his or her data or computer potential to create perils in the offline world as weapons like Barnfire were to destroy or "brick" the hospital as a result of a programming error, people's mobile phone could be affected.

Intelligence agencies have adopted "plausible deniability" as a guiding principle for Internet operations. To ensure they seek to make it impossible to trace the author

It's a stunning approach with which the digital spy agencies undermine the very foundations of the rule of law. The "plausible deniability" approach threatens to transform the Internet into a playground for superpowers and their secret services operate at the whims with very few ways to hold them accountable.

## NSA Docs on Malware and Implants

**CSEC document about the recognition of trojans and anomalies**

**The formalized process through which analysts choose requirements and then get to know the tools that can be used. QUANTUMTHEORY is a set of technologies allowing interference attacks on TCP/IP connections (including DAREDEVIL)**

**Sample code of a malware program from the Five Eyes**

Attribution is difficult and requires considerable forensics. In the new documents there are at least a few pointers. One is a keylogger that was part of the Snowden archive. It is software designed to surreptitiously intercept all data sent by the victim and record them for later inspection. It is indeed rather dated, keylogger. Similar software is used in numerous applications, so it doesn't seem to pose a threat, but the sourcecode contained in it does reveal so much. They suggest that this keylogger might be part of a set of modules that belong to the Warriorpride program. The Esperanto software used by all the Five Eyes parties was even able to break into iPhones, among other things. Documents published by SPIEGEL include sample code of a keylogger to foster further research and enable the development of appropriate defenses.

## 'Just a Bunch of Hackers'

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

responsible for covert operations. S321 employees on the third floor of one of the main buildings on the NSA campus. A report from the Snowden archive, an NSA memo from 2005, when they got started, the ROC people were "just a group of people. 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 our data. Our equipment is our equipment."

---

## NSA Docs on Exfiltration

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

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

[Presentation on the FASHIONCLEFT protocol that uses trojans to 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 data from active operations and passive signals intelligence](#)

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

---

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

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

**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 recommen

Tweet 599

 +16  
Recommend this



---

## Comments

Discuss this issue with other readers!

Share your opinion!

## Share your thoughts

Please register to add a comment.

Subject

Comment

---

### Endpoint Threat Detection

 [ziften.com/new-451-research/](http://ziften.com/new-451-research/)

New 451 Research -Endpoint Security Get Endpoint Protection Now

### Retire On \$1300 Per Month

 [liveandinvestoverseas.com](http://liveandinvestoverseas.com)

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

### Safe Step® Walk-In Tubs

 [safesteptub.com/Free-Estimates](http://safesteptub.com/Free-Estimates)

Bathe Safely And Easily Again! BBB Member. Includes Install & We

### Is He Cheating On You?

 [spokeo.com/Cheating-Spouse-Search](http://spokeo.com/Cheating-Spouse-Search)

Enter His Email Address. See Hard To Find Pics & Social Profiles N

### Want to Live in Colombia?

 [internationalliving.com](http://internationalliving.com)

Free report for people considering Visiting or Living in Colombia

### Cheap Airline Tickets

 [cheapoair.com/Call@1-888-516-7925](http://cheapoair.com/Call@1-888-516-7925)

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

### Concealed Carry Guide

 [usconcealedcarry.net](http://usconcealedcarry.net)

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

### Usd Canadian Dollar

 [wallstreetdaily.com/Top-Currencies](http://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

© SPIEGEL ONLINE 2015

All Rights Reserved

Reproduction only allowed with the permission of SPIEGELnet GmbH

---

## 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

**OVERVI**

---

**Home Politik Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft Gesundheit einestages Uni Rei**

#### 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