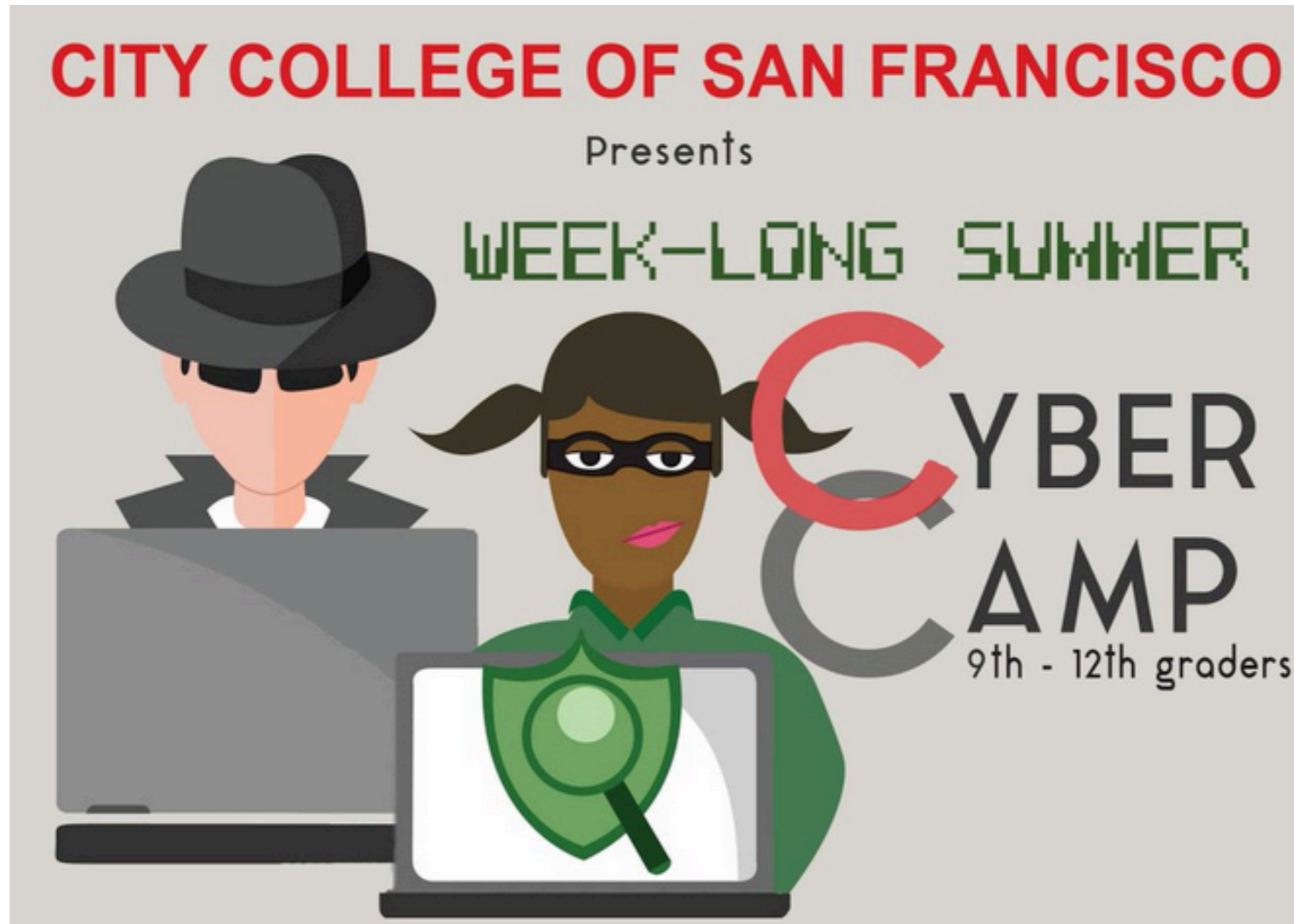


# Cyberwar & Splunk Demonstration



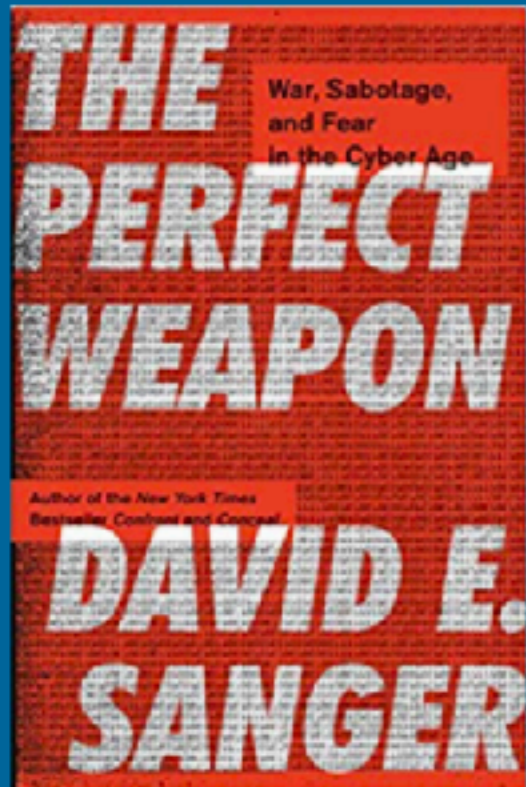
Sam Bowne

# Twitter

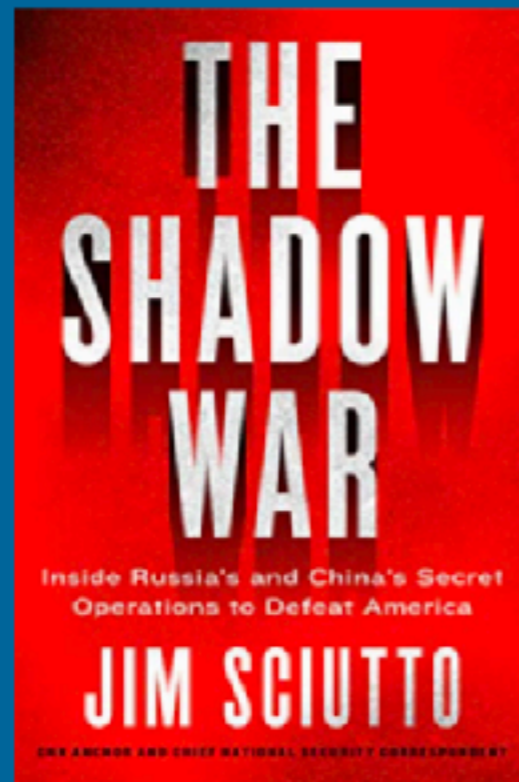


A screenshot of a Twitter profile card for Sam Bowne. The card features a circular profile picture of a man with glasses and a purple t-shirt. To the right of the picture, the name 'Sam Bowne' and the handle '@sambowne' are displayed. Below this, three statistics are shown: 'Tweets' with a value of '75.1K', 'Following' with a value of '1,733', and 'Followers' with a value of '15.7K'. The background of the card is split into a blue top half and a white bottom half.

<b>Tweets</b>	<b>Following</b>	<b>Followers</b>
<b>75.1K</b>	<b>1,733</b>	<b>15.7K</b>



Optional

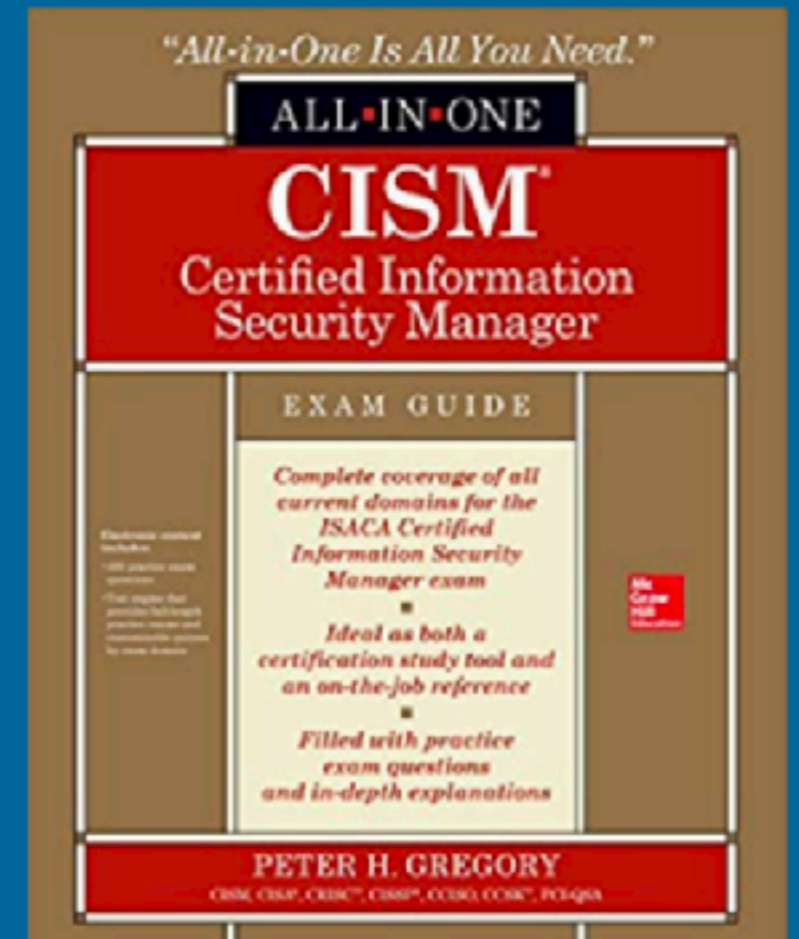


Optional

## CNIT 160: Cybersecurity Responsibilities

Fall 2019 Sam Bowne

[Schedule](#) · [Lectures](#) · [Projects](#) ·  
[Links](#) · [Home Page](#)



Required



## Official Blog

Insights from Googlers into our products, technology, and the Google culture

### A new approach to China

January 12, 2010

Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a security incident—albeit a significant one—was something quite different.

First, this attack was not just on Google. As part of our investigation we have discovered that at least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media and chemical sectors—have been similarly targeted. We are currently in the process of notifying those companies, and we are also working with the relevant U.S. authorities.

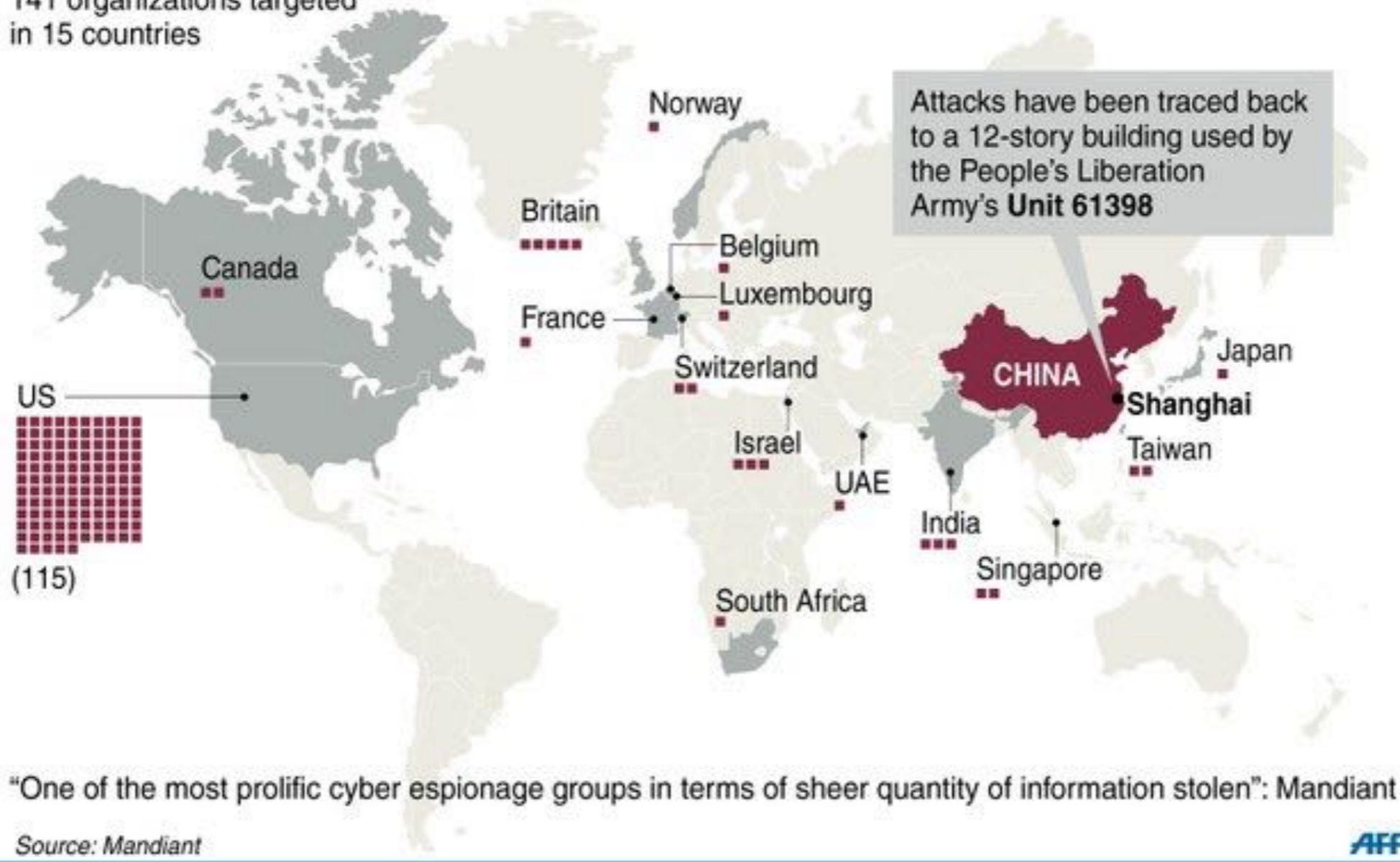
Second, we have evidence to suggest that a primary goal of the attackers was accessing the Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe their attack did not achieve that objective. Only two

# China cyberattack

US firm Mandiant has issued a 74-page report on a global cyber espionage campaign by what it says is a Chinese government-backed organization dubbed APT1 (Advanced Persistent Threat 1)

## APT1 global attacks since 2006

141 organizations targeted  
in 15 countries



- <https://www.rfa.org/english/news/china/hacking-02222013121848.html>

# Kill Chain



## APT groups [ edit ]

### American advanced persistent threat groups [ edit ]

- [Equation Group](#)<sup>[28]</sup>

### Chinese advanced persistent threat groups [ edit ]

- [PLA Unit 61398](#) (also known as APT1)
- [PLA Unit 61486](#) (also known as APT2)
- [Buckeye](#) (also known as APT3)<sup>[29]</sup>
- [Red Apollo](#) (also known as APT10)
- [PLA Unit 78020](#) (also known as APT 30)
- [Periscope Group](#) (also known as APT40)

### Iranian advanced persistent threat groups [ edit ]

- [Elfin Team](#) (also known as APT33)
- [Helix Kitten](#) (also known as APT34)

### North Korean advanced persistent threat groups [ edit ]

- [Reaper Group](#) (also known as APT37)
- [Lazarus Group](#) (also known as APT38)

### Russian advanced persistent threat groups [ edit ]

- [Fancy Bear](#) (also known as APT28)
- [Cozy Bear](#) (also known as APT29)

# The biggest cybersecurity threats to the US



## CHINA

Once launched noisy attacks, but is now more subtle.

### Notable attack:

Chinese military officers stole secrets on fighter jets, including the F-35, from Lockheed Martin.



## RUSSIA

America's most sophisticated cyber adversary.

### Notable attack:

The plot to interfere in the 2016 US presidential election by the Internet Research Agency.



## IRAN

There has been significant uptick in cyber attacks in recent years.

### Notable attack:

Iranian Behzad Mesri charged with hacking into HBO, leaking "Game of Thrones" scripts and demanding \$6 million in ransom.



## NORTH KOREA

High on US watchlist despite better diplomatic relations.

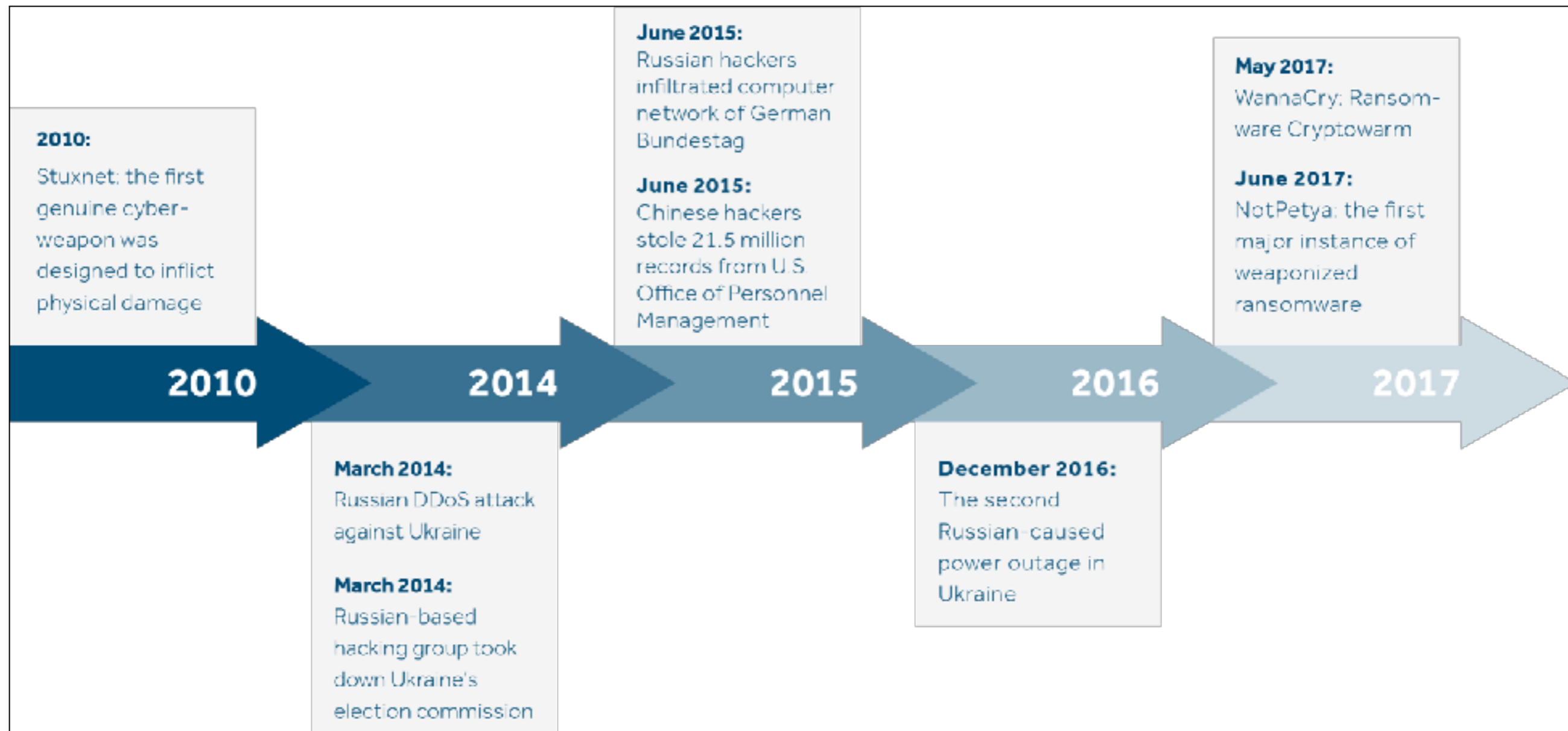
### Notable attack:

The US blamed North Korea for the WannaCry attack in 2017.

Insider Inc.



# A Brief History of Cyberwarfare

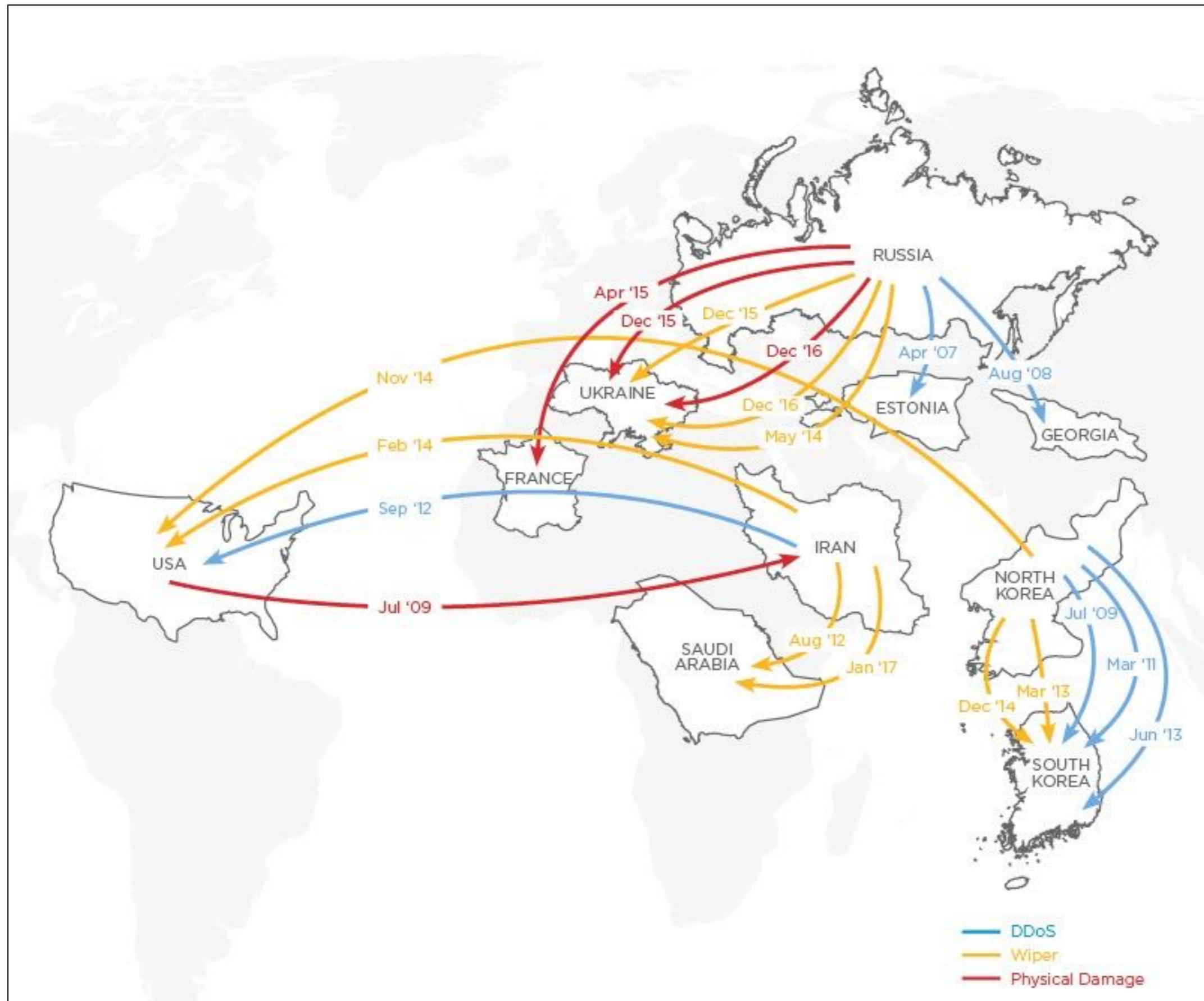


- <https://graquantum.com/a-brief-history-of-cyberwarfare/>

# Scorecard



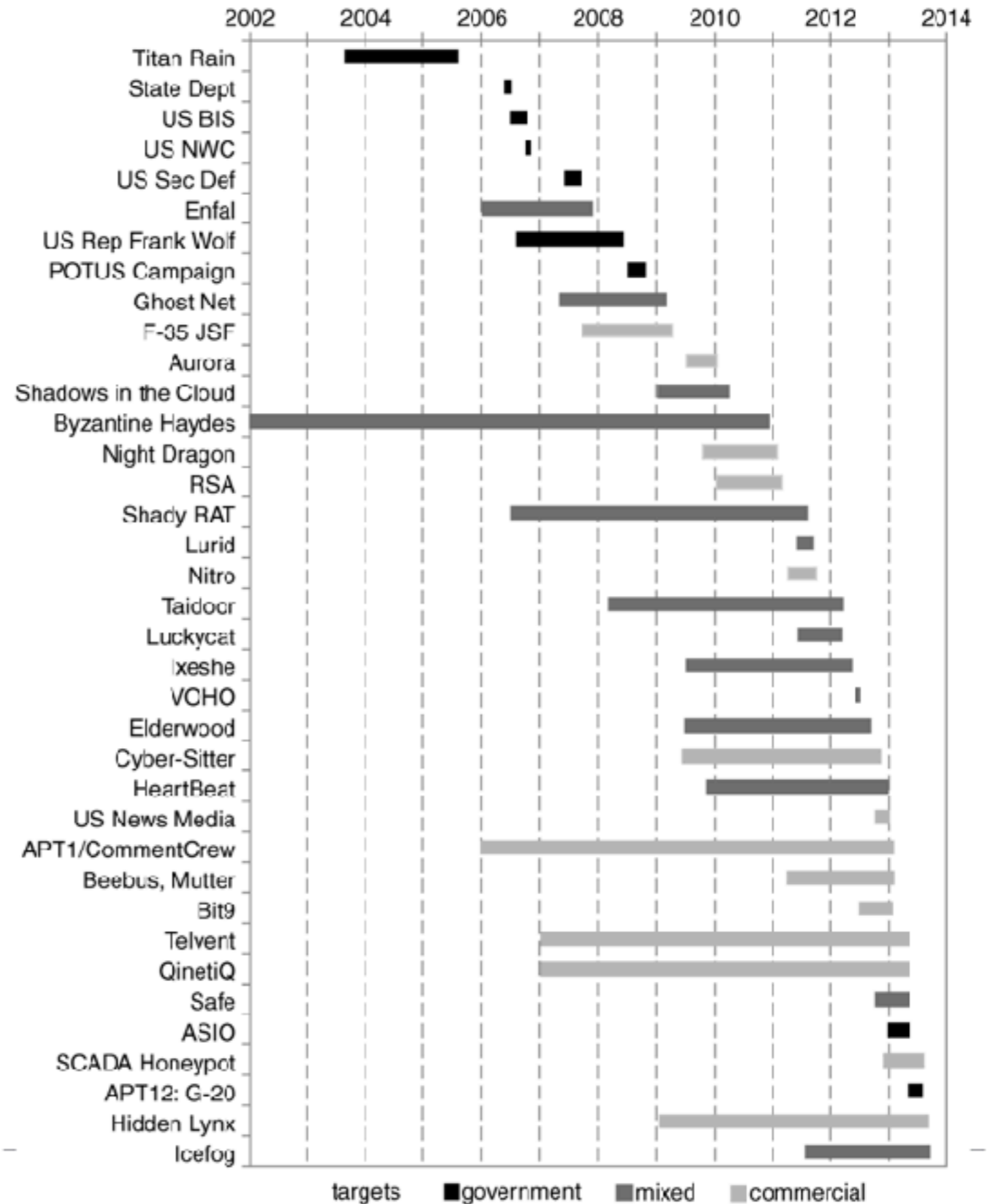
- <https://warontherocks.com/2017/07/cyber-attacks-whos-keeping-score/>



- <https://warontherocks.com/2017/07/cyber-attacks-whos-keeping-score/>

# Chinese Attacks

Figure 2. Public Reporting on Chinese Intrusions, Ordered by Reporting Date and Displaying Estimated Duration



# **THE CHINA RULES**

**I mean, there are two kinds of big companies in the United States. There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese.**

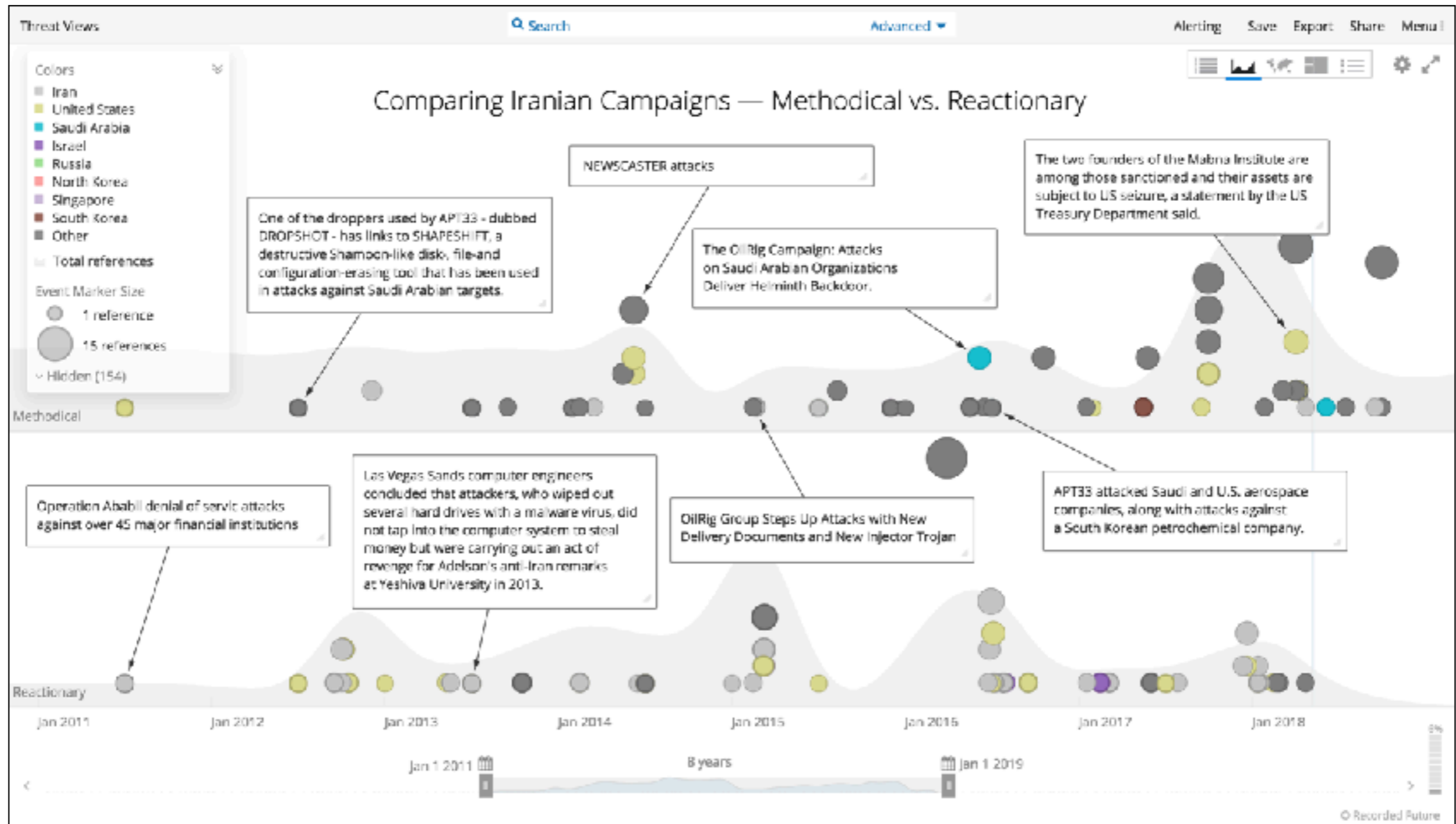
***—James Comey, then FBI director, October 5, 2014***

---

# Russian Cyberattacks



# Iranian Attacks



<https://www.recordedfuture.com>

🔄 ⓘ 🔒 <https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html>

TECHNOLOGY

The New York Times

***A Cyberattack in Saudi  
Arabia Had a Deadly Goal.  
Experts Fear Another Try.***





# *Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute*



The cyberattack on a Saudi petrochemical plant was the first known attempt to manipulate an emergency-shutdown system, which is designed to avoid disaster and protect human lives. Christophe Viseux for The New York Times

# THE SHADOW WAR

Inside Russia's and China's Secret  
Operations to Defeat America

**JIM SCIUTTO**

CNN ANCHOR AND CHIEF NATIONAL SECURITY CORRESPONDENT

# Russian Attacks



**2006:** Litvineko poisoned in London with Polonium-210

**2007:** Cyberattack on Estonia

**2008:** Invasion of Georgia

**2016:** Cyberattacks to influence US election

**2018:** Skripal poisoned with Novichok nerve agent in Salisbury, England



Hillary Clinton and Sergei Lavrov with the "reset" button Clinton presented to Lavrov in March, 2009

# Dan Coats Lost His Job for Telling Trump the Truth

The president wants intelligence that will hurt his enemies, not challenge his opinions.

By FRED KAPLAN

JULY 29, 2019 • 1:47 PM



Opinions

# Mitch McConnell is a Russian asset




Senate Majority Leader Mitch McConnell (R-Ky.) speaks to reporters on Capitol Hill in Washington on Tuesday. (Susan Walsh/AP)

# US Attack Tools

# STUXNET, THE WORLD'S FIRST DIGITAL WEAPON



Iranian President Mahmoud Ahmadinejad during a tour of centrifuges at Natanz in 2008.  OFFICE OF THE PRESIDENCY OF THE ISLAMIC REPUBLIC OF IRAN

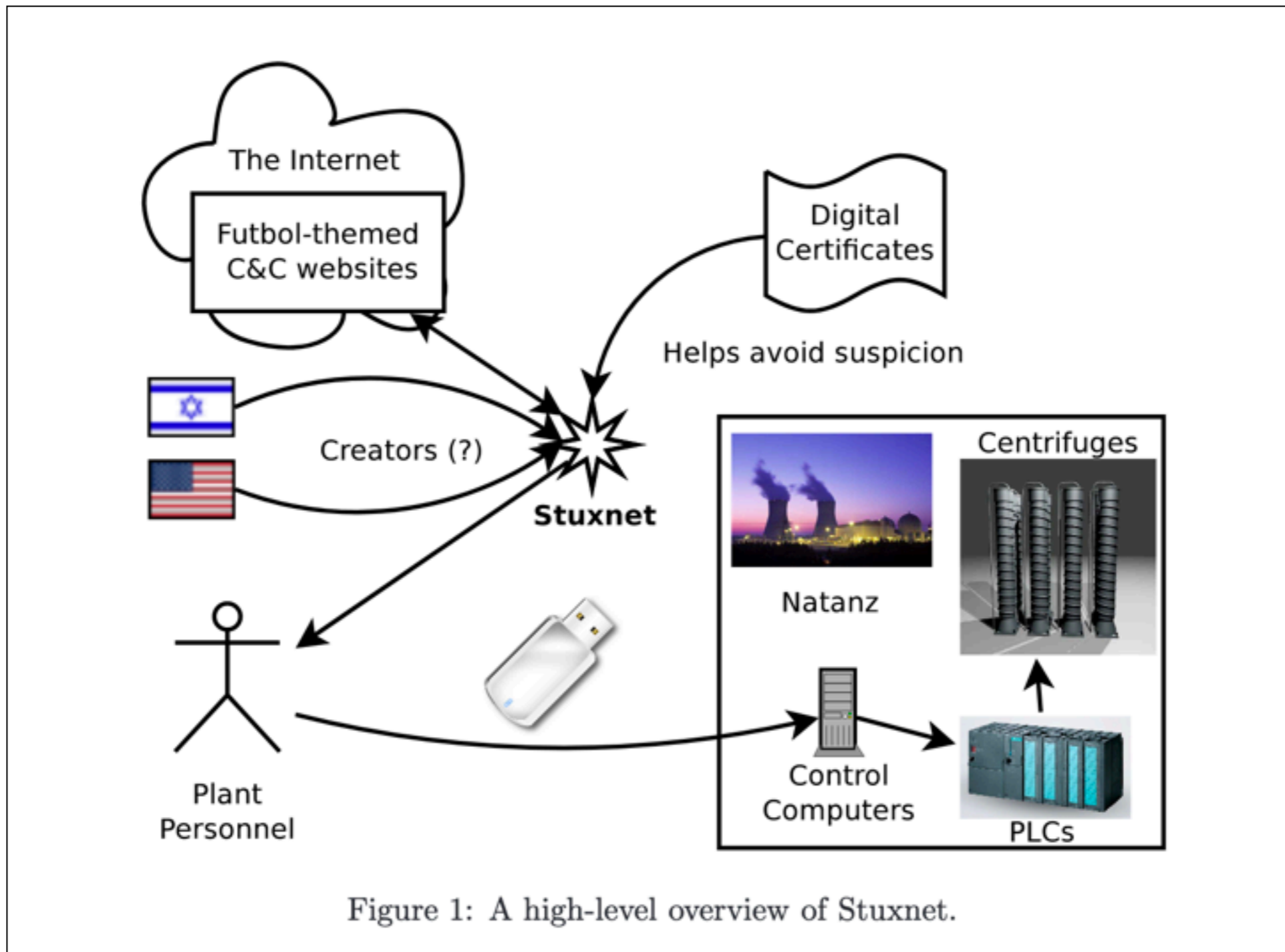


This recent undated satellite image provided by Space Imaging/Inta SpaceTurk shows the once-secret Natanz nuclear complex in Natanz, Iran, about 150 miles south of Tehran.

 AP PHOTO/SPACE IMAGING/INTA SPACETURK. HQ

<https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>





<https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf>

## 2.3 Command and Control servers

After Stuxnet establishes itself on a computer, it tries to contact one of two servers via HTTP:

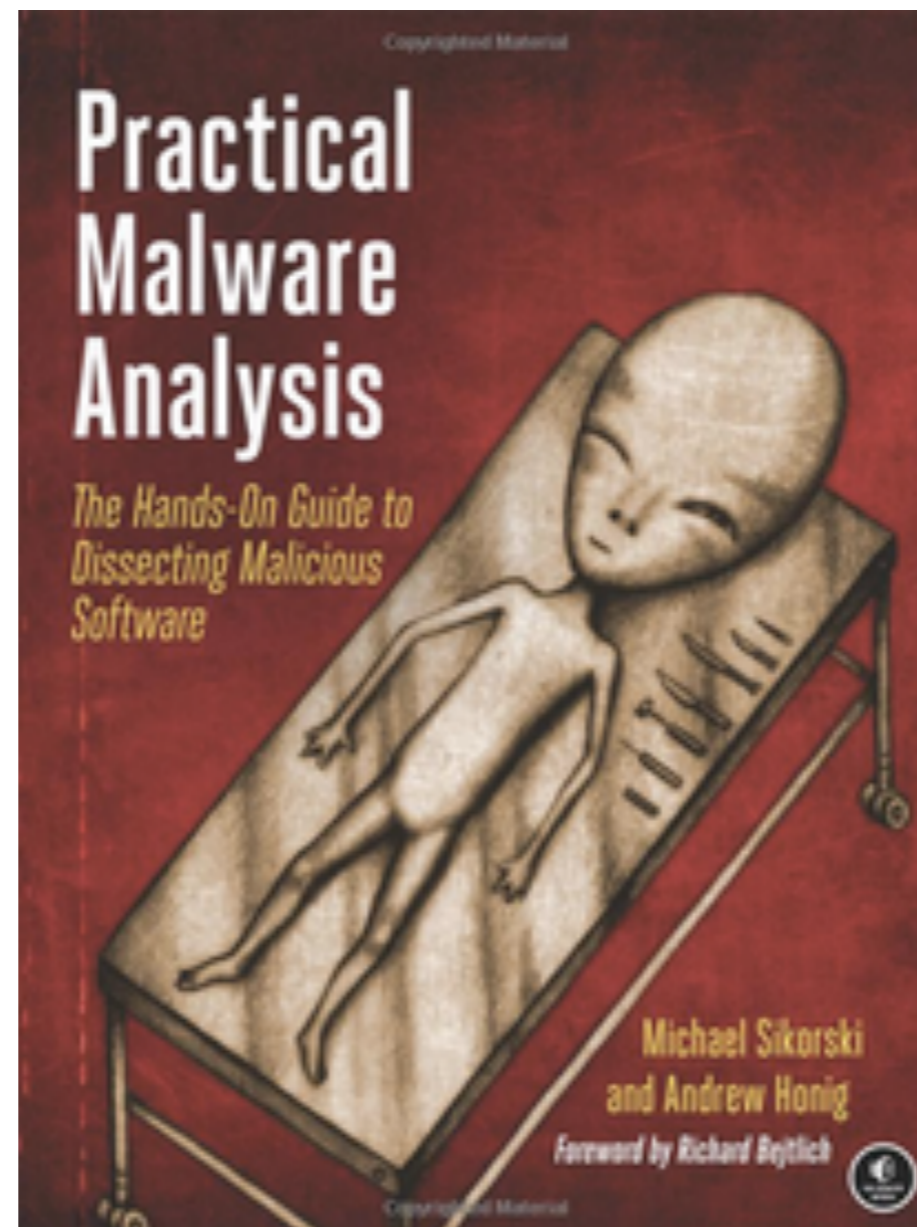
- [www.mypremierfutbol.com](http://www.mypremierfutbol.com)
- [www.todaysfutbol.com](http://www.todaysfutbol.com)

### 2.4.2 Kernel-Mode

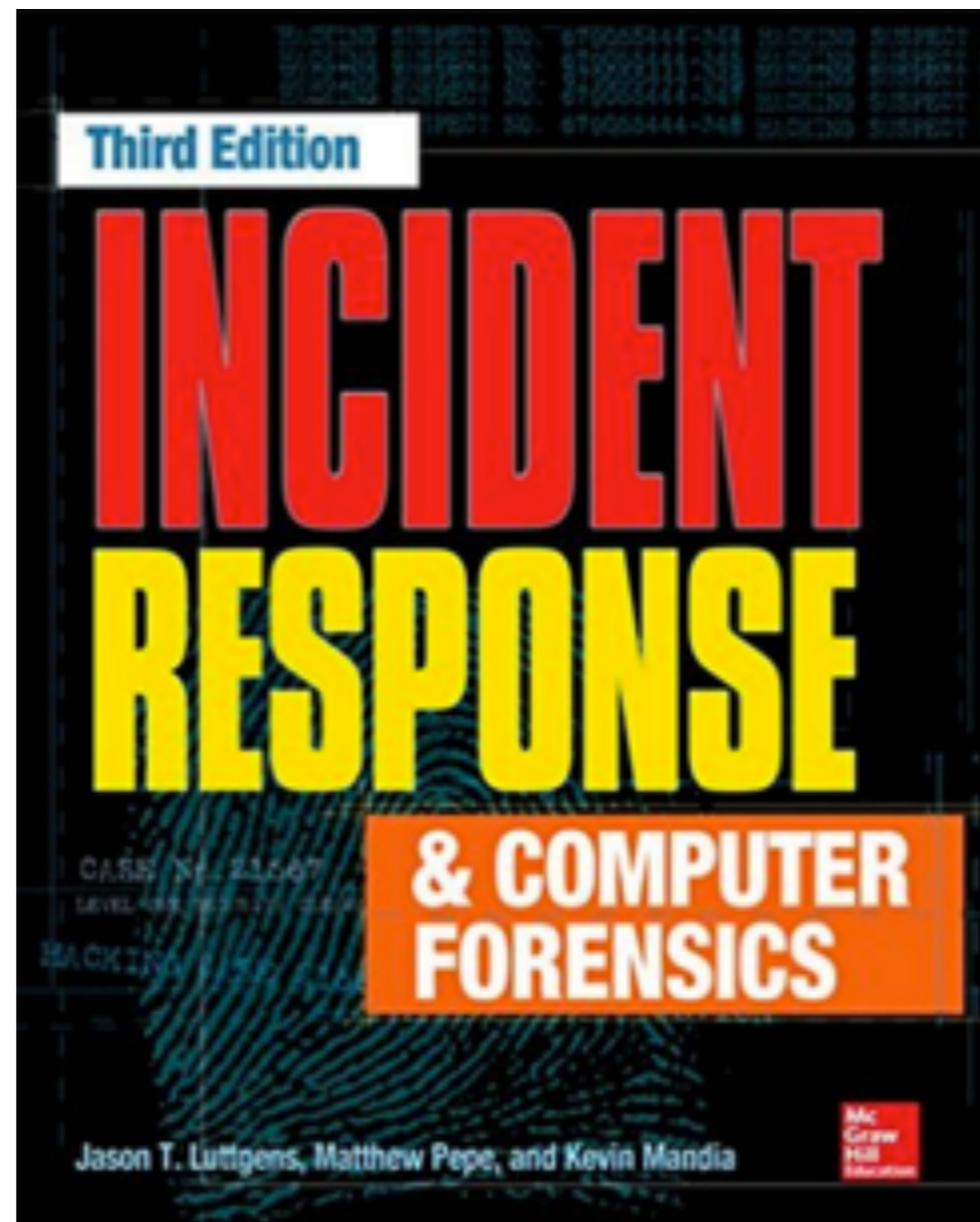
Stuxnet installs two kernel-mode drivers. `Mrxcls.sys` is a driver signed by a Realtek certificate as shown in Figure 6. When Stuxnet wants to install it onto the system, it marks it as a boot startup so it starts in the early stages of Windows boot. This driver first reads a registry key which has been written in the installation step and contains the information for injecting Stuxnet images into certain processes.

The other driver, `Mrxnet.sys`, is actually the rootkit and is also digitally signed by a Realtek certificate. It creates a device object and attaches it to the system's device objects so that it can monitor all requests sent to these objects. The purpose of this job is to hide files which meet certain criteria from users.

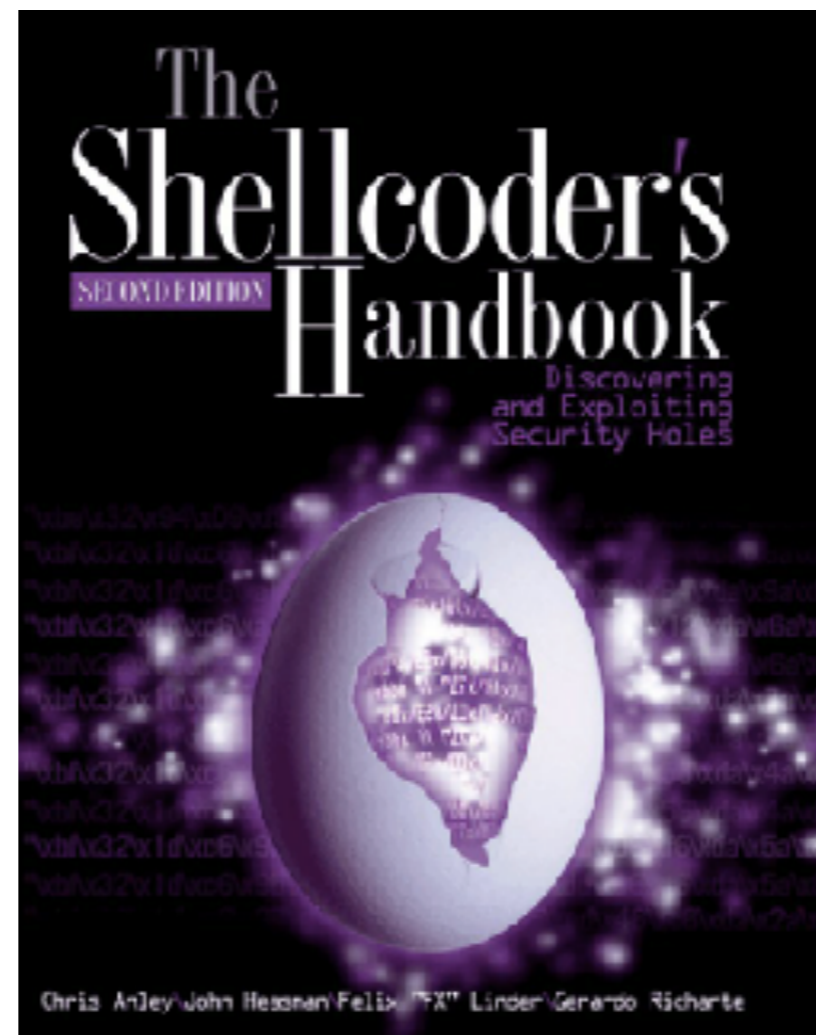
# CNIT 126: Practical Malware Analysis



# CNIT 152: Incident Response



# CNIT 127: Exploit Development



# CNIT 50: Network Security Monitoring



🏠 ↻ ⓘ 🔒 <https://samsclass.info/50/proj/purple-bots.htm> 120% ⋮ 🛡️ ☆ 📄 🔍 🚫 🗑️

## Purple Team 4: Threat Hunting with Splunk (325 pts)

[Scores from Pacific Hackers 5-11-19](#)