State sponsored offensive cyber-attacks

Stephen McCombie

NHL STENDEN

university of applied sciences

About Me

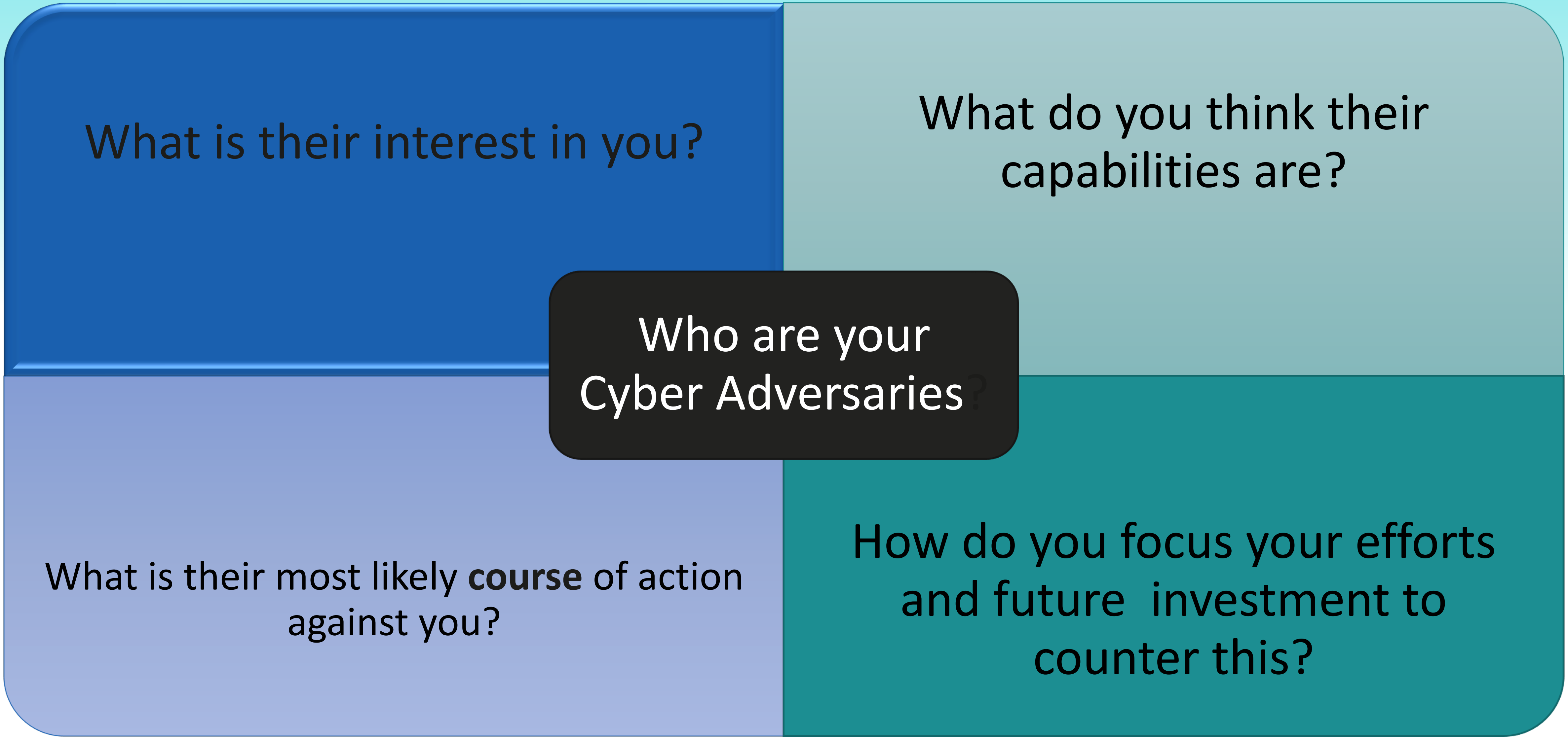
- Over 20 years working in cyber security
- Worked in law enforcement, academia and industry
- PhD in Computer Science - Thesis examined Russian and Ukrainian cybercrime groups that targeted Australian Banks in early 2000s
- Research interests include maritime cyber threats, cyber threat intelligence, state sponsored offensive cyber and information warfare

RSA SECURITY™

National Australia Bank

IBM

NSW Police Force



Who are your Cyber Adversaries?

What is their interest in you?

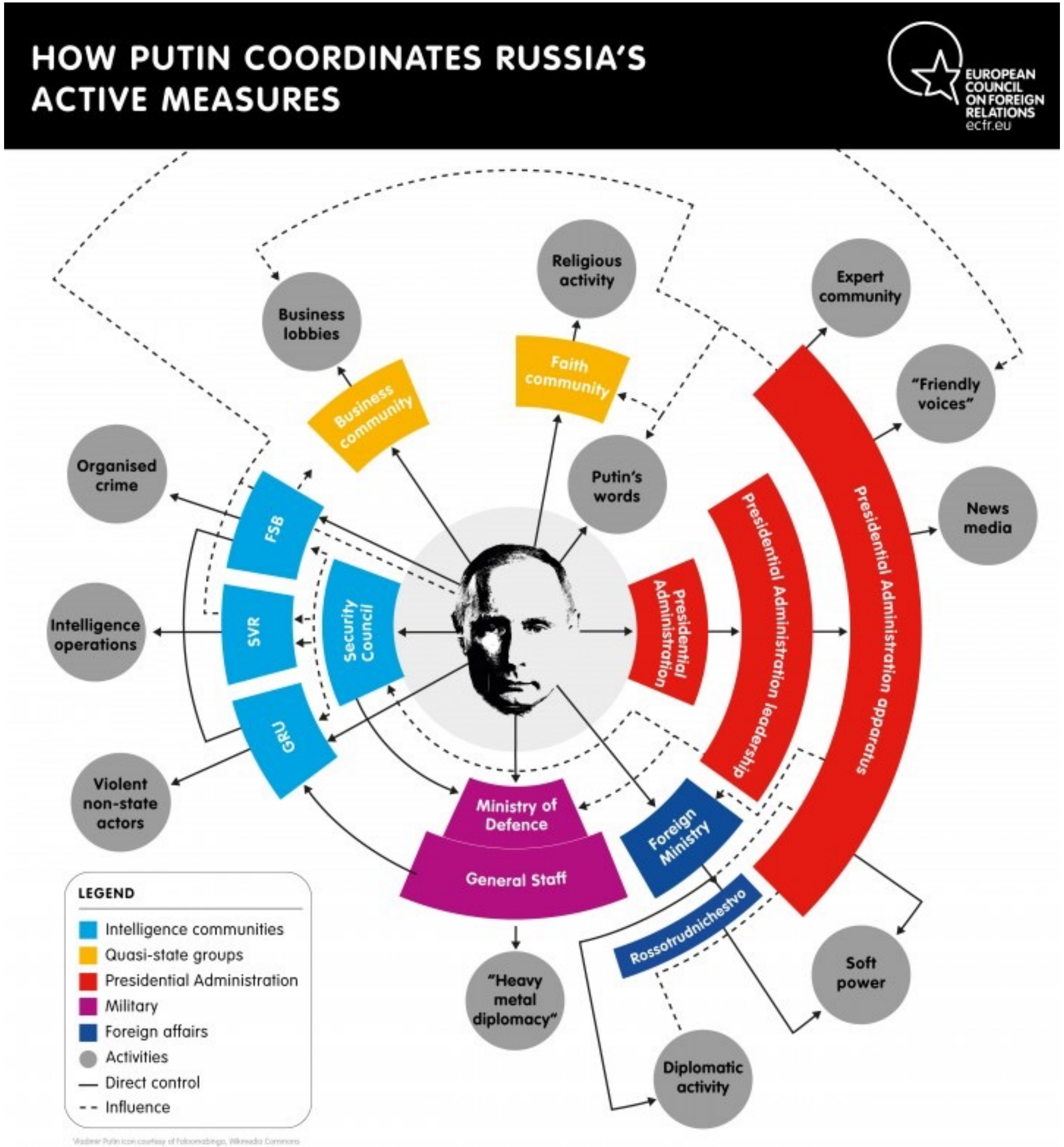
What do you think their capabilities are?

What is their most likely **course** of action against you?

How do you focus your efforts and future investment to counter this?

State sponsored offensive cyber-attacks

- Hydrid warfare (seen in war in Ukraine)
- Achieve same aims by many means (cyber just one)
- Cyber is a new domain of warfare (Land/Sea/Air/Space)
- But Cyber seems somehow short of war on its own
- Russian/China not alone in using its offensive capabiltiy
- New “cold war” will feature these types of cyber attacks



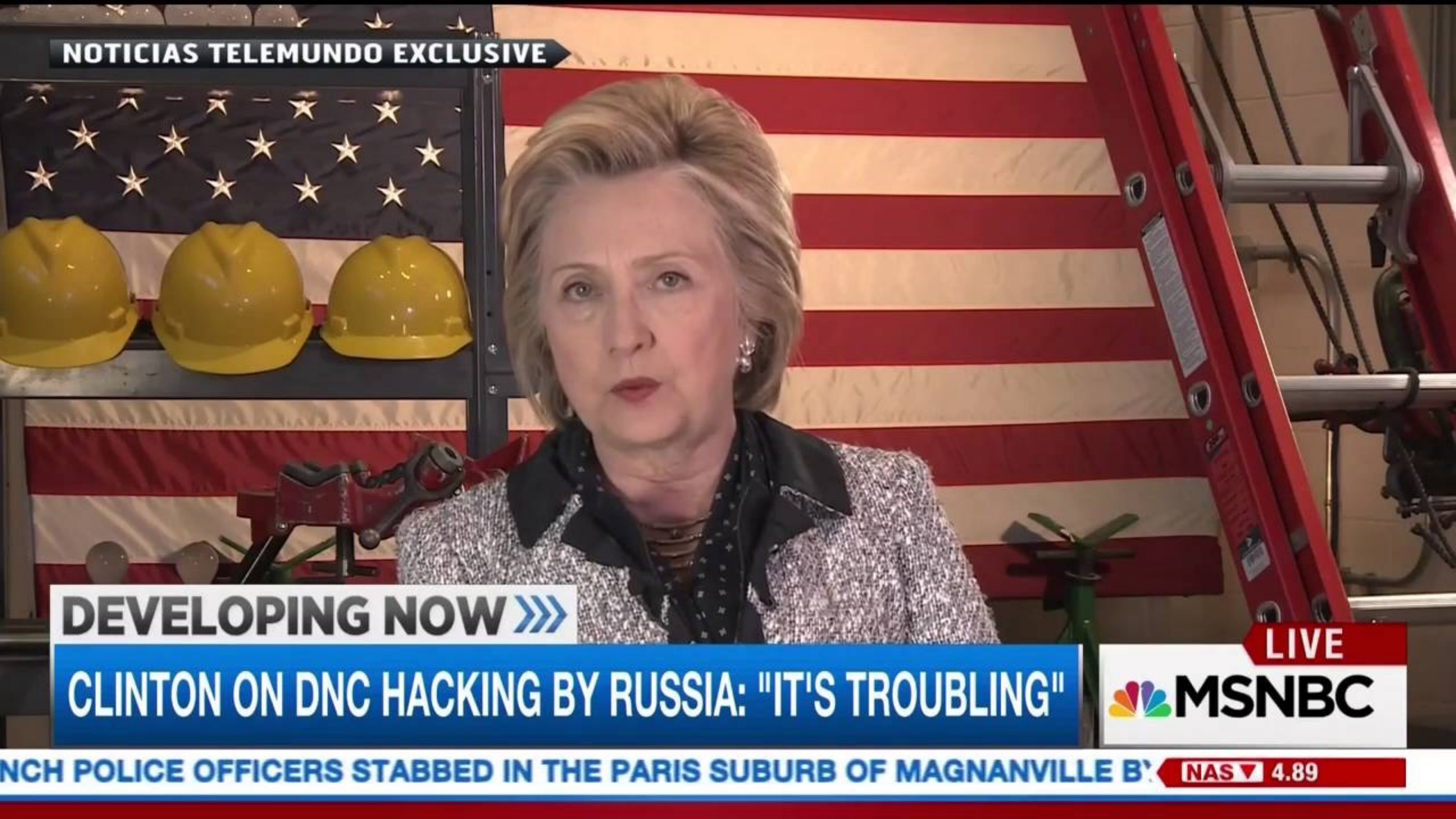
(Source: Galeotti 2018)

Russia: Legacy of KGB

- The current State Security apparatus of Russia is in many ways the descendant of the Soviet Unions’ KGB.
- Indeed its style of operation and even some of its personnel have not changed
- Russia’s “secret police” have a long history dating back to the large and surprisingly effective Tsarist Okhrana.

KGB Active Measures (The Mitrokhin Archive)

- The KGB sought to influence the course of world events by a variety of ‘active measures’ (aktivinyye meropriatia) ranging from media manipulation to ‘special actions’ involving various degrees of violence.
- Throughout the Cold War the United States was the main target for KGB active measures as well as for intelligence collection. Most were at the non-violent end of the active measures spectrum – ‘influence operations’ designed to discredit the Main Adversary.



NOTICIAS TELEMUNDO EXCLUSIVE

DEVELOPING NOW

CLINTON ON DNC HACKING BY RUSSIA: "IT'S TROUBLING"

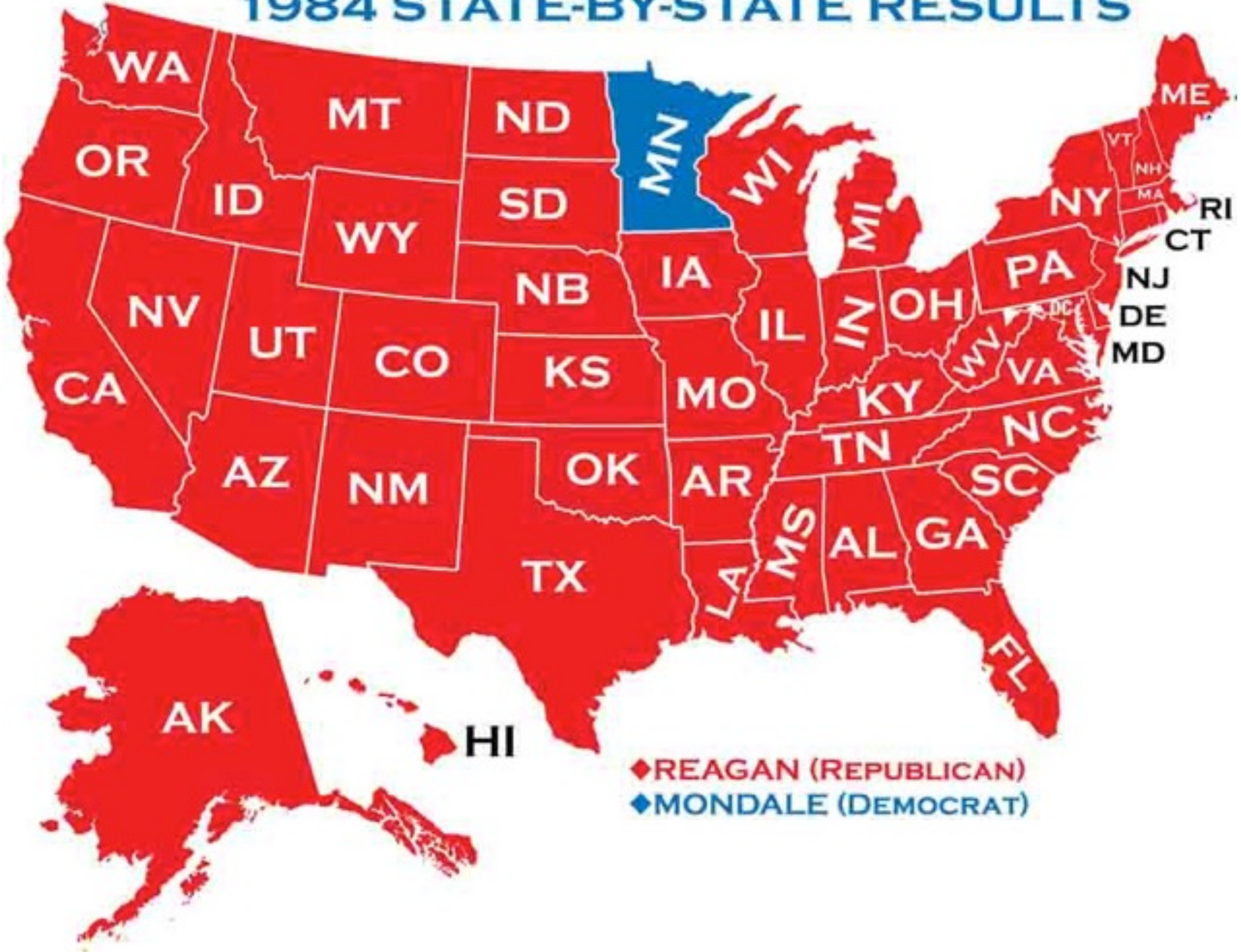
NCH POLICE OFFICERS STABBED IN THE PARIS SUBURB OF MAGNANVILLE BY

any talk about our influencing the outcome of the U.S. election is all lies.

KGB Operations against US Elections 1984 (The Mitrokhin Archive)

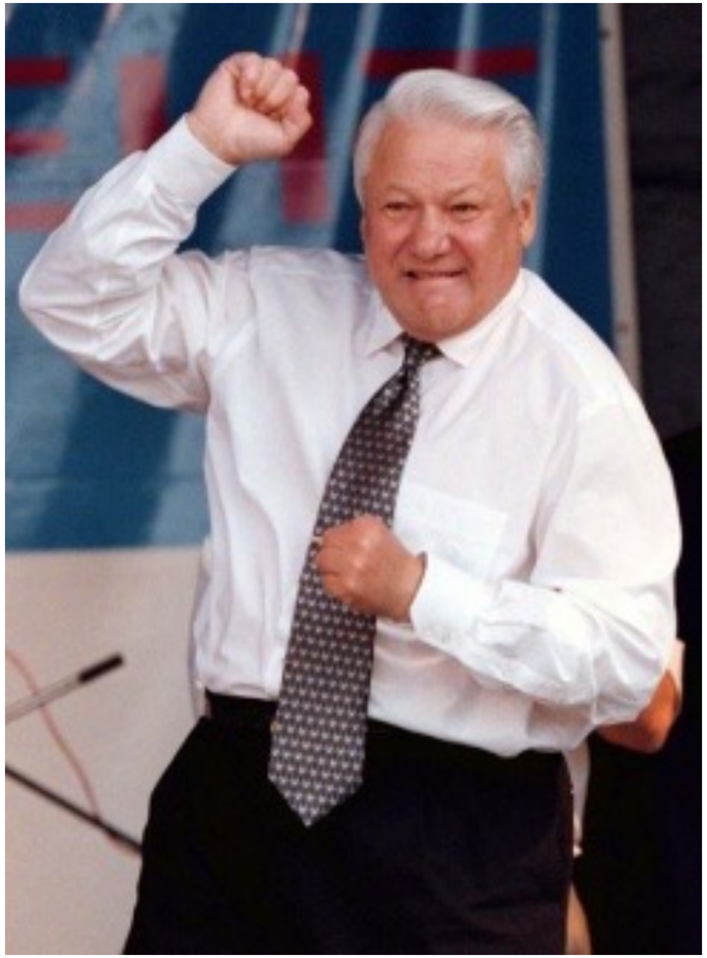
- On 25 February 1983 the Centre (KGB Headquarters) instructed its three American residencies to begin planning active measures to ensure Reagan's defeat in the presidential election of November 1984
- The Centre made clear that any candidate, of either party, would be preferable to Reagan.
- Active measures 'theses' in domestic policy included Reagan's alleged discrimination against ethnic minorities; corruption in his administration; and Reagan's subservience to the military-industrial complex

1984 STATE-BY-STATE RESULTS



KGB Dissolved 1991 (Galeotti 2017)

- In one of his many toxic legacies, former Russian President Boris Yeltsin ignored calls to disband the KGB that appeared beyond repair and rebuild it from scratch.
- Instead, after 1991, he opted to partition the KGB. Its first chief directorate, responsible for espionage, was simply rebranded as the Foreign Intelligence Service (SVR).
- Most of the directorates tasked with domestic security were gathered together first under the umbrella of the Ministry of Security, then the Federal Counter-Intelligence Service, and, in 1995, the FSB.



KGB Alumni

Roles of Russia‘s intelligence community

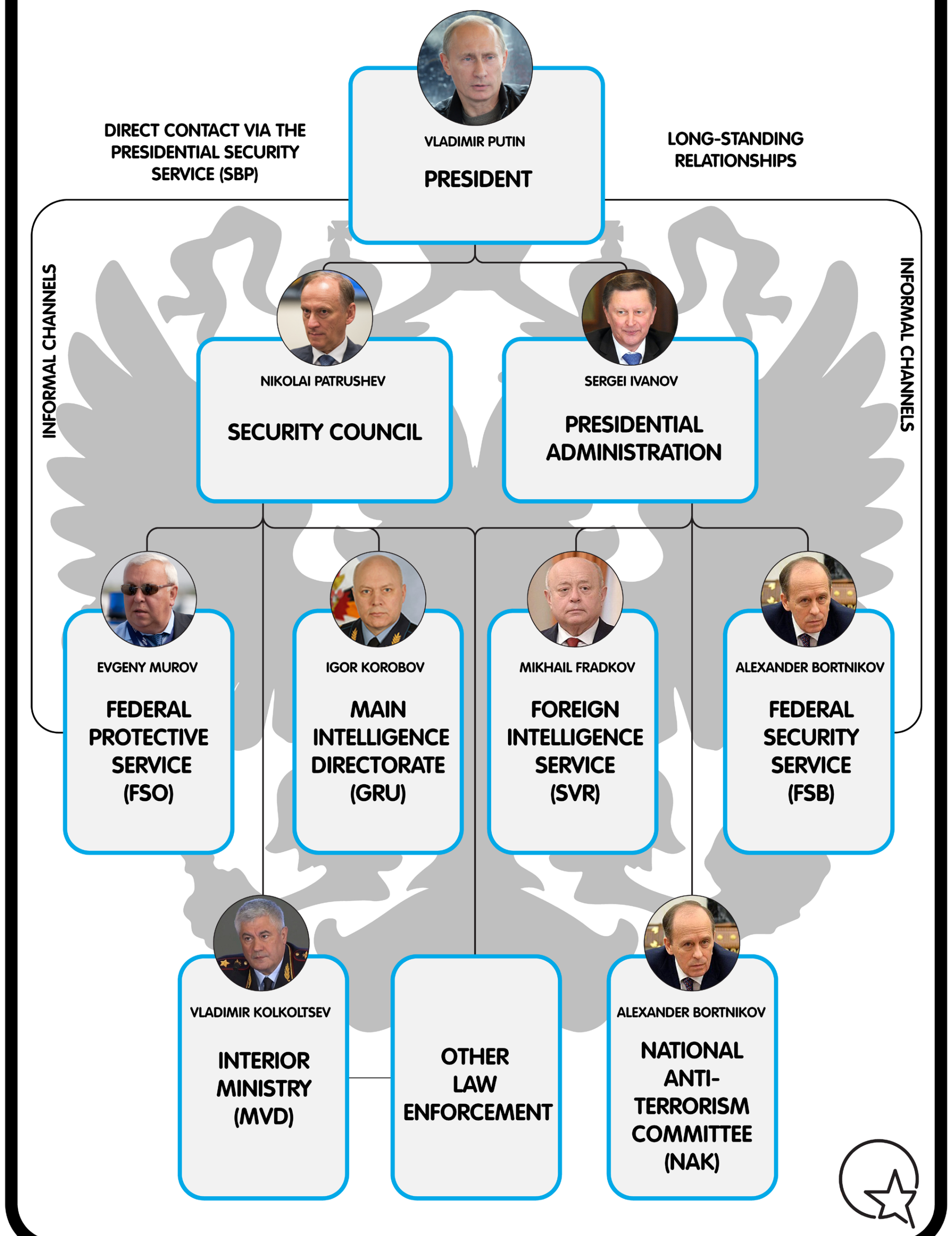
	Political intelligence	Economic intelligence	Military intelligence	Active measures	Counter -intelligence	Political security	Law enforcement
Federal Security Service (FSB)	○			○	●	●	○
Foreign Intelligence Service (SVR)	●	●	○	●	○	○	
Main Intelligence Directorate (GRU)	○	○	●	●	○		
Federal Protection Service (FSO)					○	●	○
Interior Ministry (MVD)					○	○	●
Prosecutor General’s Office (GP)						○	●
Investigatory Committee (SK)						●	●
The Federal Anti-Drug Service (FSKN)		○					●
National Anti-Terrorism Committee (NAK)					○	●	●
Soviet KGB	●	●	○	●	●	●	○

● Main role

○ Subsidiary role

(Source: Galeotti 2018)

Russia's intelligence architecture



DIRECT CONTACT VIA THE PRESIDENTIAL SECURITY SERVICE (SBP)

VLADIMIR PUTIN

PRESIDENT

LONG-STANDING RELATIONSHIPS

INFORMAL CHANNELS

NIKOLAI PATRUSHEV

SECURITY COUNCIL

SERGEI IVANOV

PRESIDENTIAL ADMINISTRATION

INFORMAL CHANNELS

EVGENY MUROV

FEDERAL PROTECTIVE SERVICE (FSO)

IGOR KOROBOV

MAIN INTELLIGENCE DIRECTORATE (GRU)

MIKHAIL FRADKOV

FOREIGN INTELLIGENCE SERVICE (SVR)

ALEXANDER BORTNIKOV

FEDERAL SECURITY SERVICE (FSB)

VLADIMIR KOLKOLTSEV

INTERIOR MINISTRY (MVD)

OTHER LAW ENFORCEMENT

ALEXANDER BORTNIKOV

NATIONAL ANTI-TERRORISM COMMITTEE (NAK)

(Source: Galeotti 2018)

Federal Security Service (FSB)

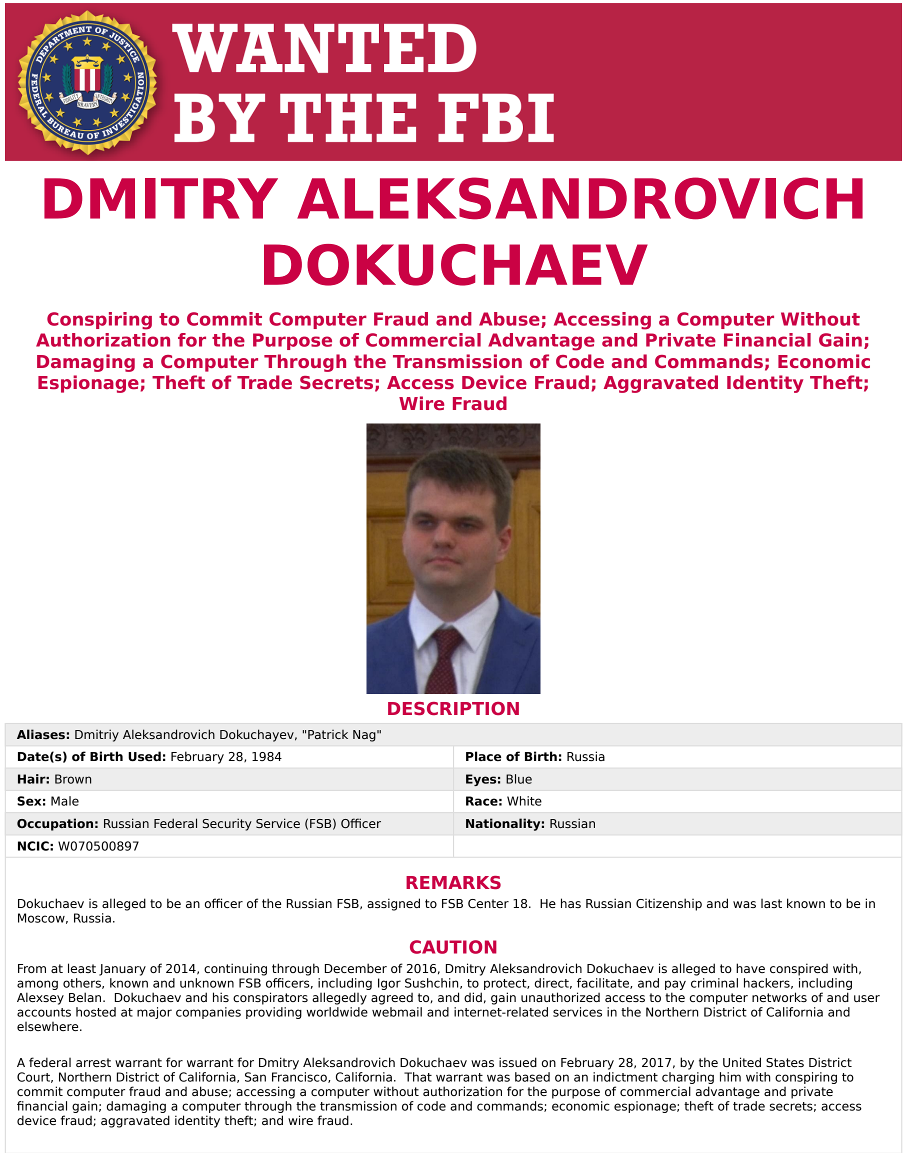
- The FSB are the best known and most politically influential of Russia's Security organisations
- Its role is the protection and defence of the state border of the Russian Federation, the protection of internal sea waters, the territorial sea, the exclusive economic zone, the continental shelf and their natural resources and ensuring the information security of Russia

Information Security Center (TsIB)

- Information Security Center (TsIB) manages computer security investigations for the Interior Ministry and the FSB. Its also known as Military Unit (Vch) 64829.

- TsIB has close links with Russia’s two main cybersecurity companies, Kaspersky and Group-IB (Galeotti 2016).

FSB Liaison in Action



WANTED BY THE FBI

DMITRY ALEKSANDROVICH DOKUCHAEV

Conspiring to Commit Computer Fraud and Abuse; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging a Computer Through the Transmission of Code and Commands; Economic Espionage; Theft of Trade Secrets; Access Device Fraud; Aggravated Identity Theft; Wire Fraud

DESCRIPTION

Aliases: Dmitriy Aleksandrovich Dokuchayev, "Patrick Nag"	
Date(s) of Birth Used: February 28, 1984	**Place of Birth:** Russia
Hair: Brown	**Eyes:** Blue
Sex: Male	**Race:** White
Occupation: Russian Federal Security Service (FSB) Officer	**Nationality:** Russian
NCIC: W070500897	

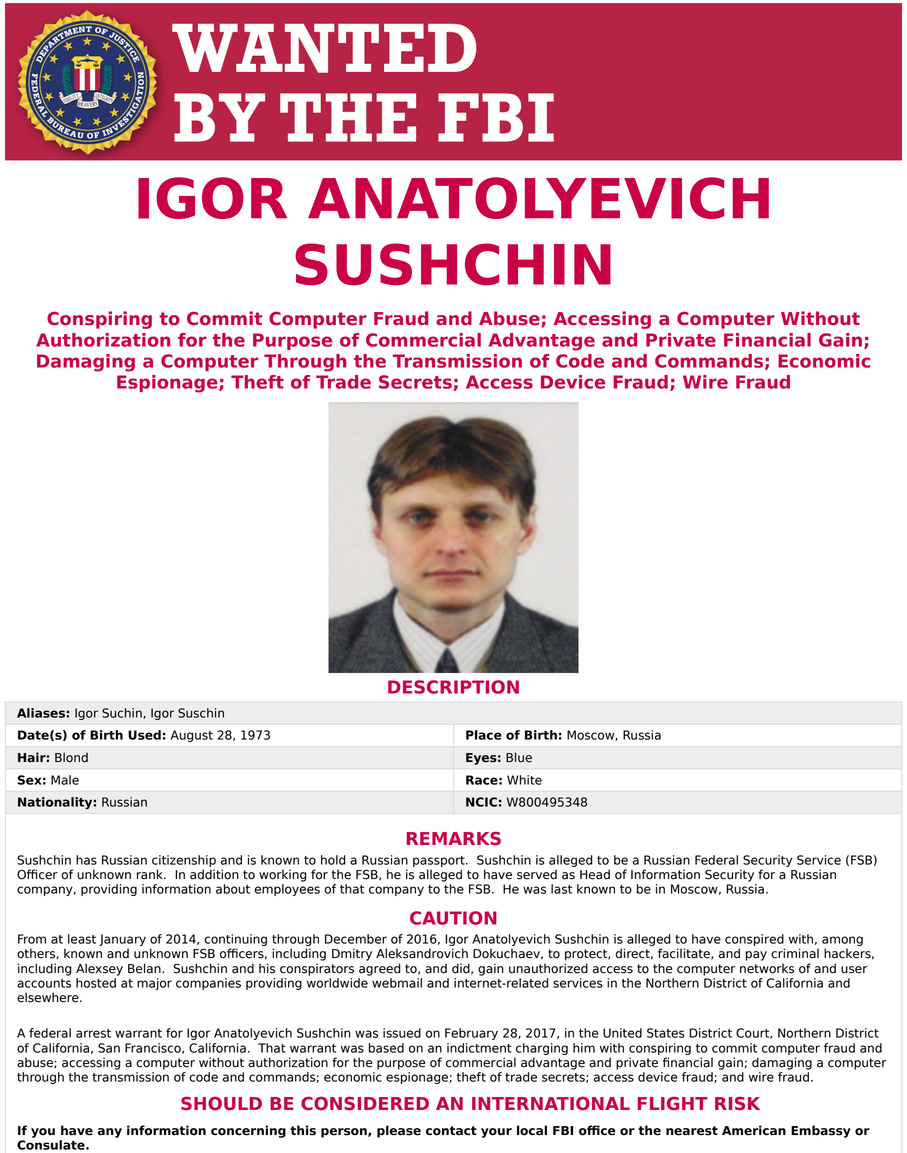
REMARKS

Dokuchaev is alleged to be an officer of the Russian FSB, assigned to FSB Center 18. He has Russian Citizenship and was last known to be in Moscow, Russia.

CAUTION

From at least January of 2014, continuing through December of 2016, Dmitry Aleksandrovich Dokuchaev is alleged to have conspired with, among others, known and unknown FSB officers, including Igor Sushchin, to protect, direct, facilitate, and pay criminal hackers, including Alexsey Belan. Dokuchaev and his conspirators allegedly agreed to, and did, gain unauthorized access to the computer networks of and user accounts hosted at major companies providing worldwide webmail and internet-related services in the Northern District of California and elsewhere.

A federal arrest warrant for warrant for Dmitry Aleksandrovich Dokuchaev was issued on February 28, 2017, by the United States District Court, Northern District of California, San Francisco, California. That warrant was based on an indictment charging him with conspiring to commit computer fraud and abuse; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging a computer through the transmission of code and commands; economic espionage; theft of trade secrets; access device fraud; aggravated identity theft; and wire fraud.



WANTED BY THE FBI

IGOR ANATOLYEVICH SUSHCHIN

Conspiring to Commit Computer Fraud and Abuse; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging a Computer Through the Transmission of Code and Commands; Economic Espionage; Theft of Trade Secrets; Access Device Fraud; Wire Fraud

DESCRIPTION

Aliases: Igor Suchin, Igor Suschin	
Date(s) of Birth Used: August 28, 1973	**Place of Birth:** Moscow, Russia
Hair: Blond	**Eyes:** Blue
Sex: Male	**Race:** White
Nationality: Russian	**NCIC:** W800495348

REMARKS

Sushchin has Russian citizenship and is known to hold a Russian passport. Sushchin is alleged to be a Russian Federal Security Service (FSB) Officer of unknown rank. In addition to working for the FSB, he is alleged to have served as Head of Information Security for a Russian company, providing information about employees of that company to the FSB. He was last known to be in Moscow, Russia.

CAUTION

From at least January of 2014, continuing through December of 2016, Igor Anatolyevich Sushchin is alleged to have conspired with, among others, known and unknown FSB officers, including Dmitry Aleksandrovich Dokuchaev, to protect, direct, facilitate, and pay criminal hackers, including Alexsey Belan. Sushchin and his conspirators agreed to, and did, gain unauthorized access to the computer networks of and user accounts hosted at major companies providing worldwide webmail and internet-related services in the Northern District of California and elsewhere.

A federal arrest warrant for Igor Anatolyevich Sushchin was issued on February 28, 2017, in the United States District Court, Northern District of California, San Francisco, California. That warrant was based on an indictment charging him with conspiring to commit computer fraud and abuse; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging a computer through the transmission of code and commands; economic espionage; theft of trade secrets; access device fraud; and wire fraud.

SHOULD BE CONSIDERED AN INTERNATIONAL FLIGHT RISK

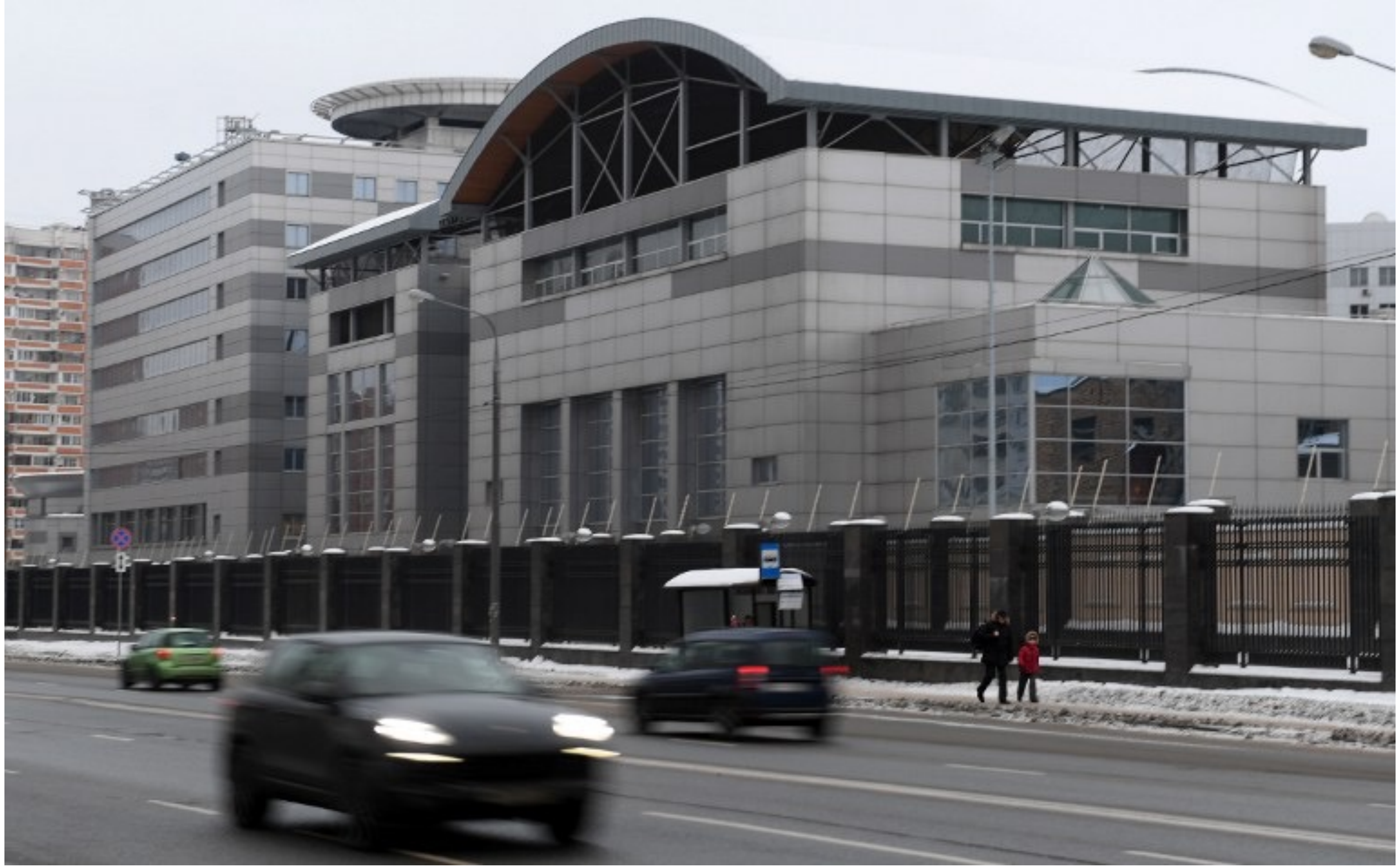
If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

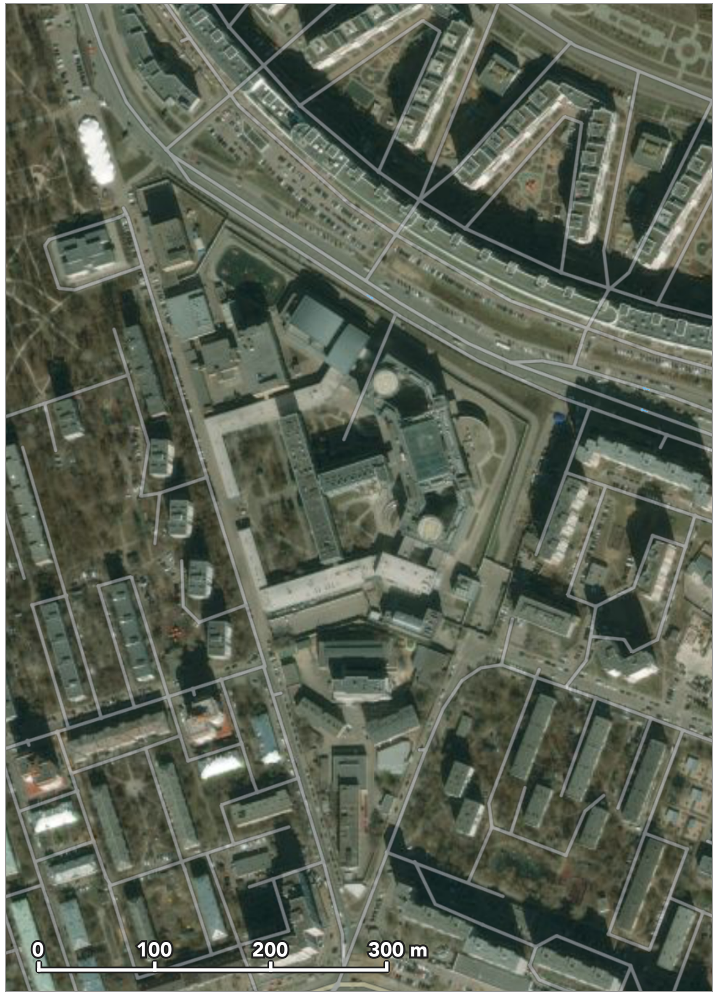
Main Intelligence Directorate (GRU)

- The GRU is Russia’s foreign military intelligence organisation.
- It is part of the Russian Military somewhat similar to the US Defence Intelligence Agency.
- It deploys six times more agents than the SVR
- It has significant technical expertise in information warfare
- They are believed to been the main perpetrators of the DNC hack

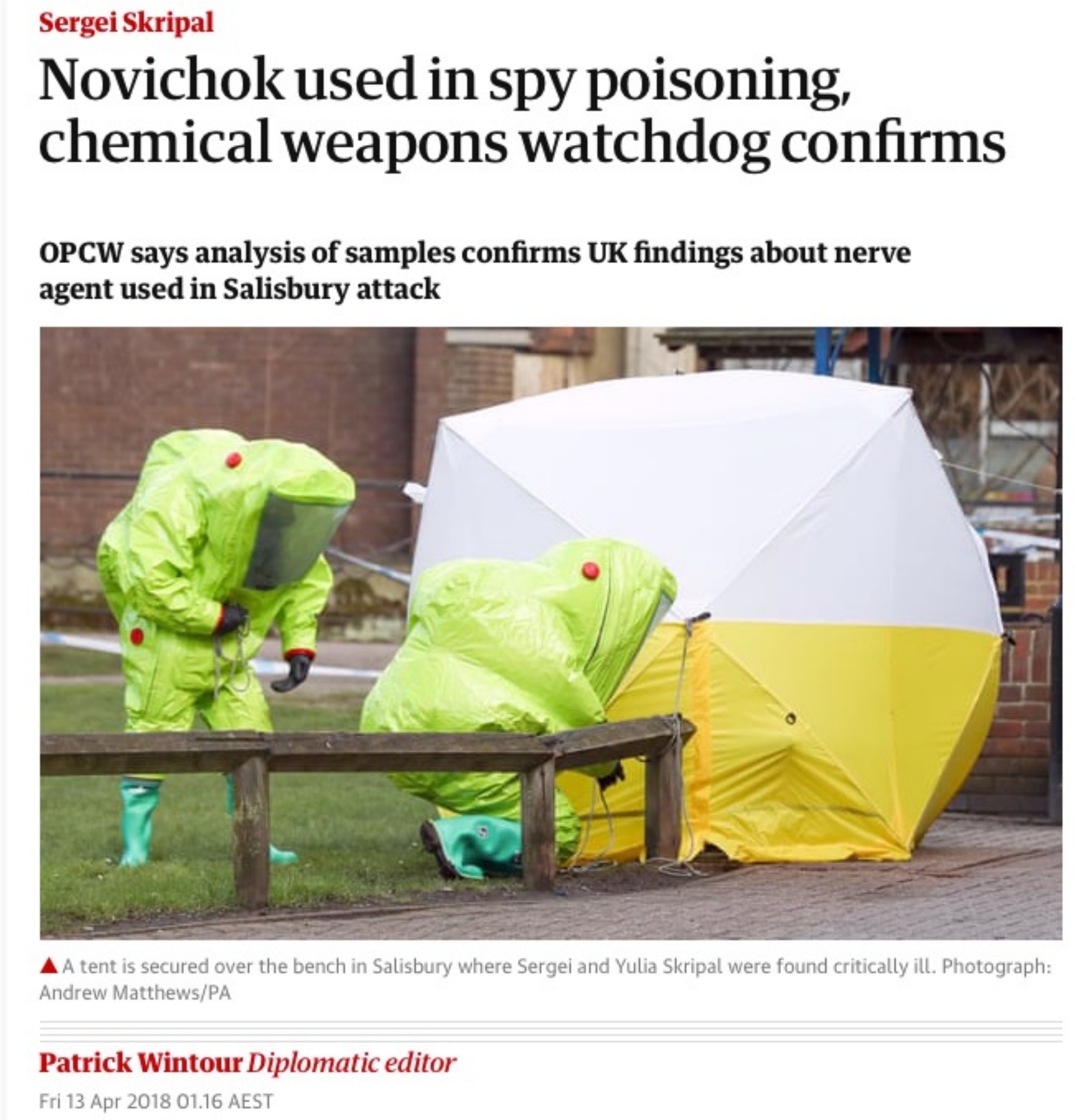
GRU Alumni

near Khoroshevskiy — Moscow





1 of 1



Sergei Skripal

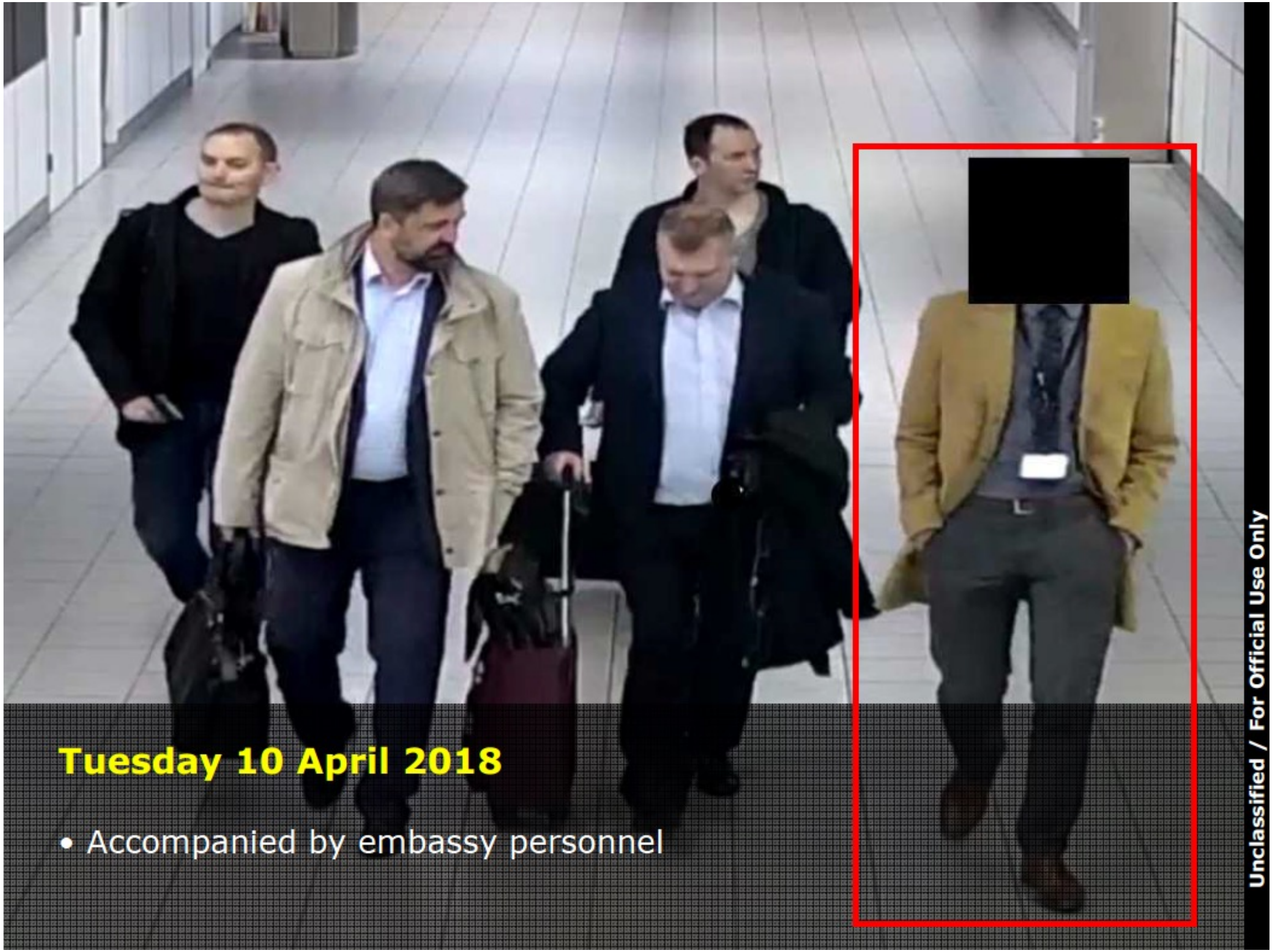
Novichok used in spy poisoning, chemical weapons watchdog confirms

OPCW says analysis of samples confirms UK findings about nerve agent used in Salisbury attack

▲ A tent is secured over the bench in Salisbury where Sergei and Yulia Skripal were found critically ill. Photograph: Andrew Matthews/PA

Patrick Wintour *Diplomatic editor*

Fri 13 Apr 2018 01.16 AEST



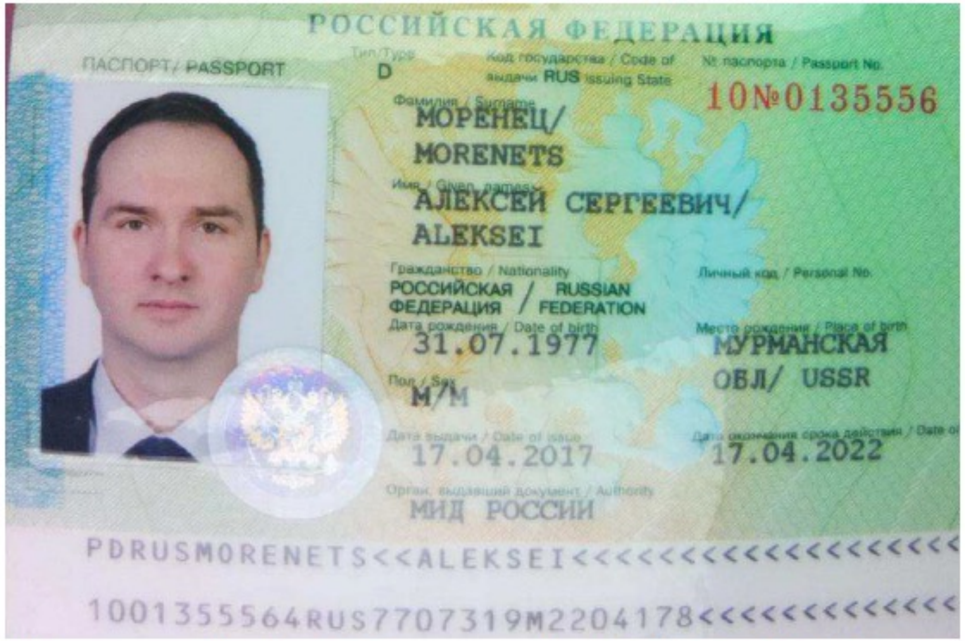
[redacted]

Tuesday 10 April 2018

- Accompanied by embassy personnel

Unclassified / For Official Use Only

Aleksei MORENETS



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ПАСПОРТ/ PASSPORT

Тип/Type
D

Код государства / Code of
выдачи RUS issuing State

№ паспорта / Passport No.
10№0135556

Фамилия / Surname
МОРЕНЕЦ/
MORENETS

Имя / Given names
АЛЕКСЕЙ СЕРГЕЕВИЧ/
ALEKSEI

Гражданство / Nationality
РОССИЙСКАЯ / RUSSIAN
ФЕДЕРАЦИЯ / FEDERATION

Личный код / Personal No.

Дата рождения / Date of birth
31.07.1977

Место рождения / Place of birth
МУРМАНСКАЯ
ОБЛ/ USSR

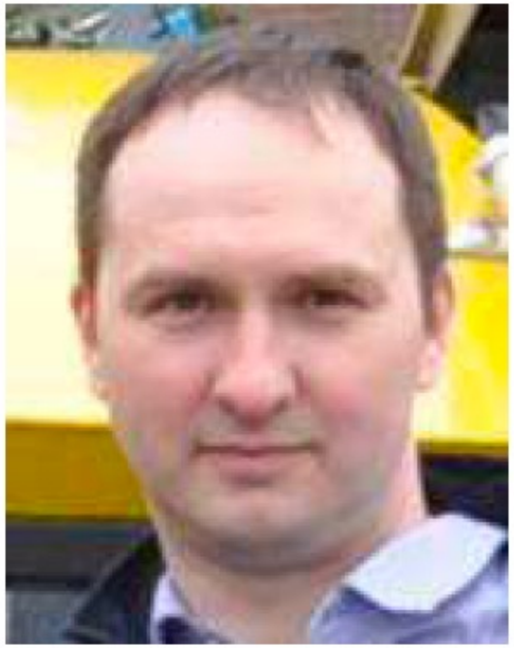
Пол / Sex
М/M

Дата выдачи / Date of issue
17.04.2017

Дата окончания срока действия / Date of
17.04.2022

Орган, выдавший документ / Authority
МИД РОССИИ

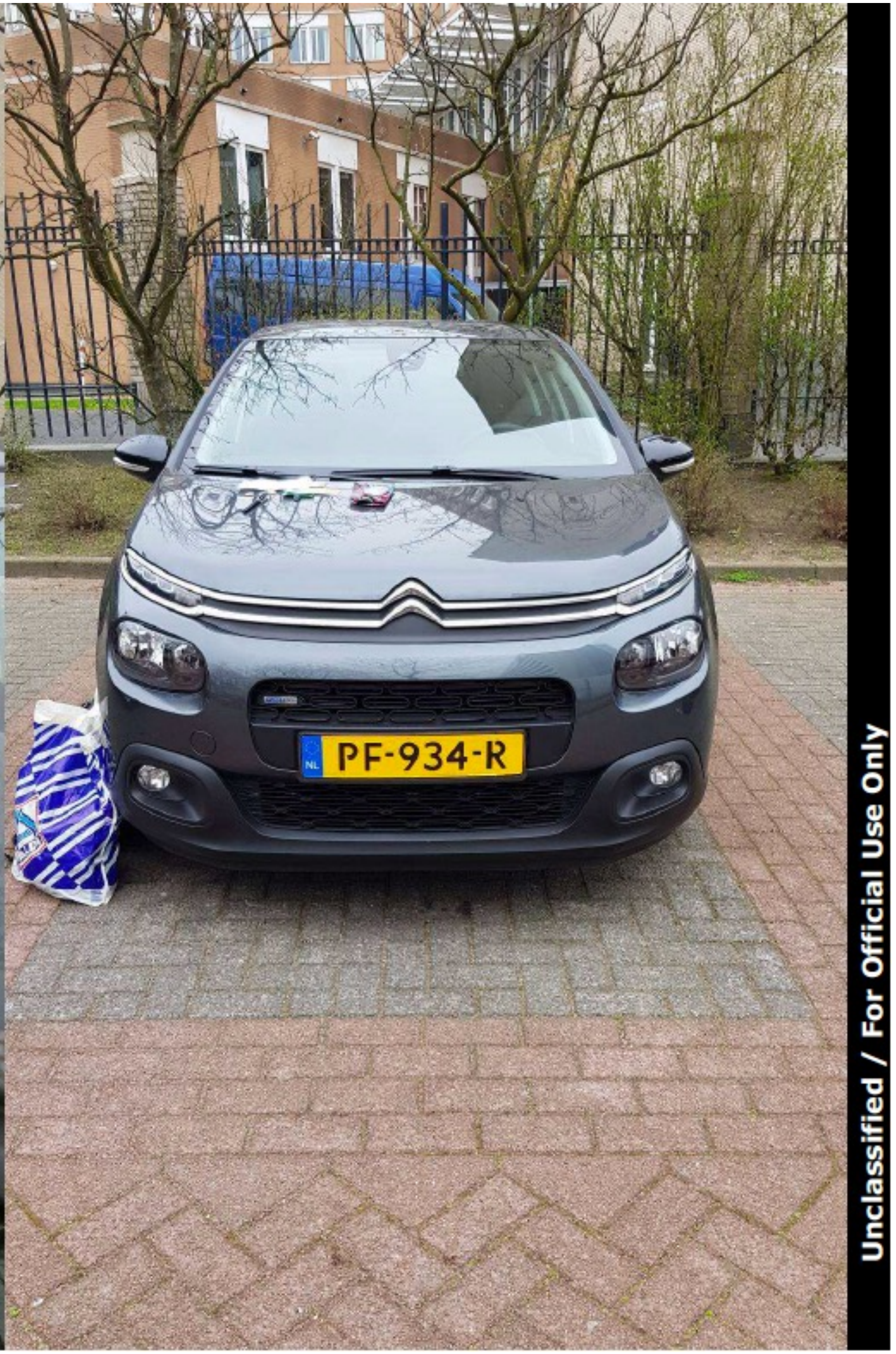
```
PDRUSMORENETS<<ALEKSEI<<<<<<<<<<<<<<<<<<<
1001355564RUS7707319M2204178<<<<<<<<<<<<<
```



Name: Aleksei Sergeyvich MORENETS
Date of birth: 31-07-1977
Place of birth: Moermanskaya Oblast
Passport nr: 100135556

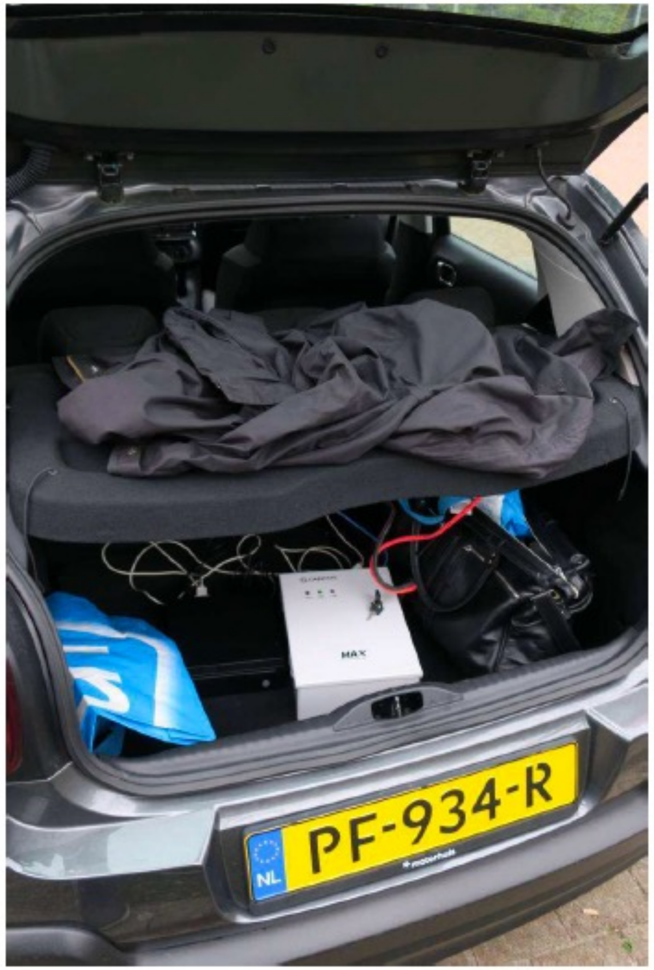
Role: Cyber operator

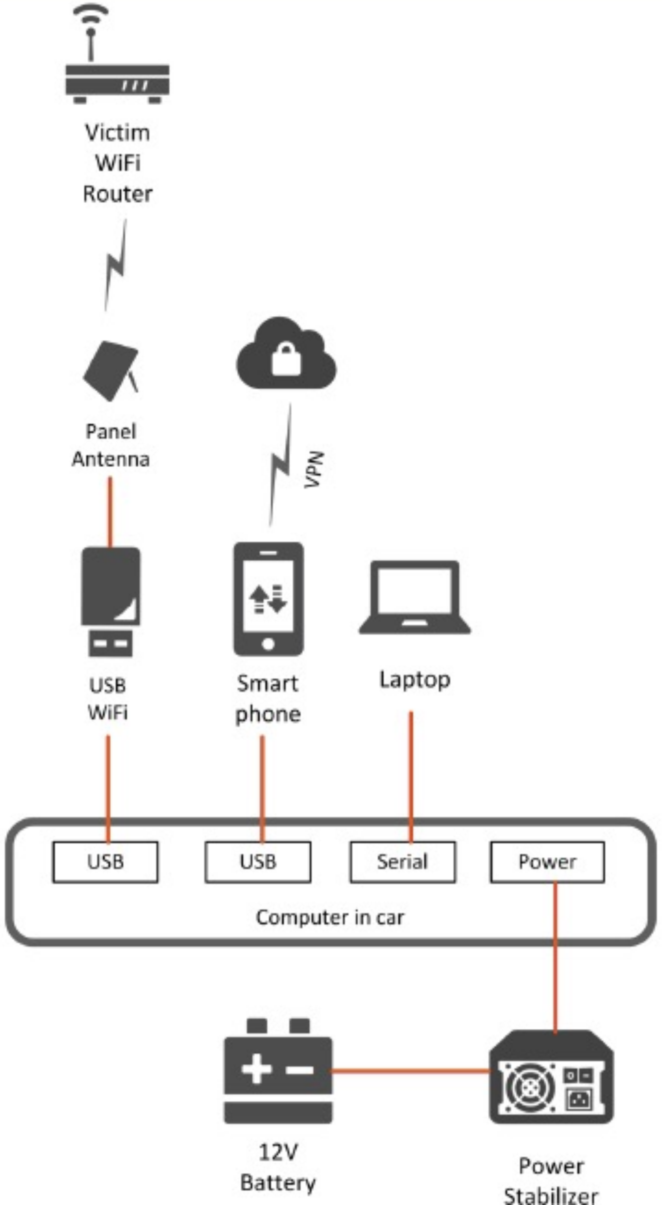
Unclassified / For Official Use Only



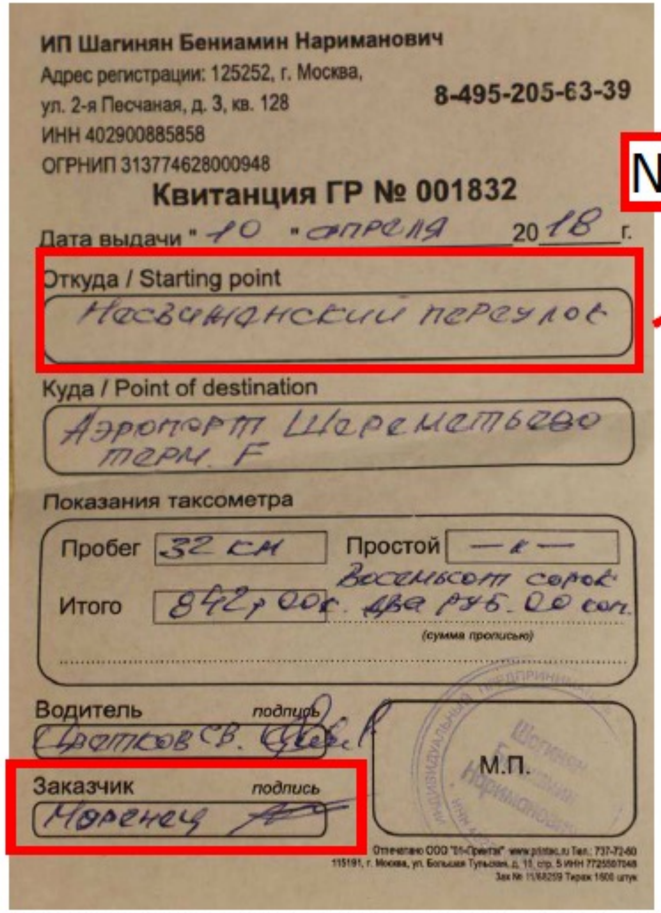
Unclassified / For Official Use Only

Schematische weergave





Unclassified / For Official Use Only



ИП Шагинян Бениамин Нариманович
Адрес регистрации: 125252, г. Москва,
ул. 2-я Песчаная, д. 3, кв. 128
ИНН 402900885858
ОГРНИП 313774628000948

8-495-205-63-39

Квитанция ГР № 001832

Дата выдачи " 10 " апреля 20 18 г.

Откуда / Starting point
Несвижанский переулок

Куда / Point of destination
Аэропорт Шереметьево
терм. F

Показания таксометра

Пробег 32 км Простой — к —

Итого 842 р 00 к. Восемьсот сорок два руб. 00 коп.
(сумма прописью)

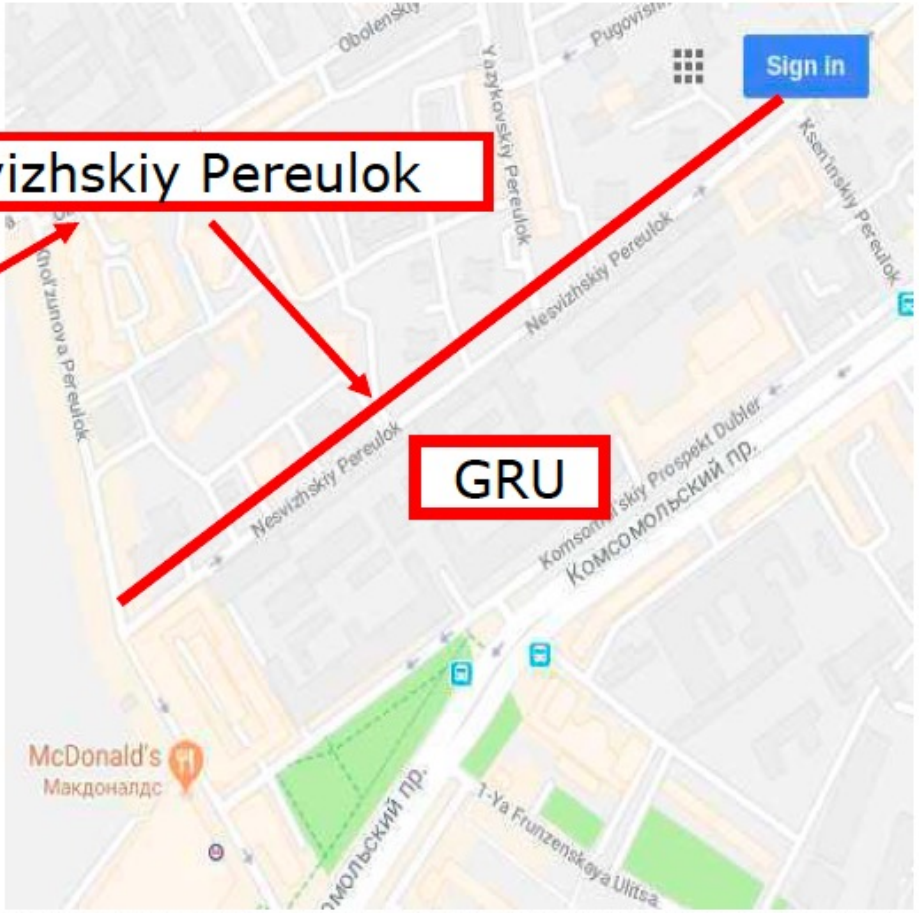
Водитель подпись
Сретков С.В.

Заказчик подпись
Моренец

М.П.

ИНДИВИДУАЛЬНЫЙ ПРЕДПРИНИМАТЕЛЬ Шагинян Бениамин Нариманович ИНН

Отпечатано ООО "Б1-Принтас" www.pistac.ru Тел.: 737-72-60
115191, г. Москва, ул. Большая Тульская, д. 11, стр. 5 ИНН 7725597048
Зак № 11/68259 Тираж 1500 штук



Nesvizhskiy Pereulok

GRU

MORENETS' taxi receipt

- From Nesvizhskiy Pereulok to Moscow Sheremetyevo airport
- Date: 10 April 2018

Unclassified / For Official Use Only

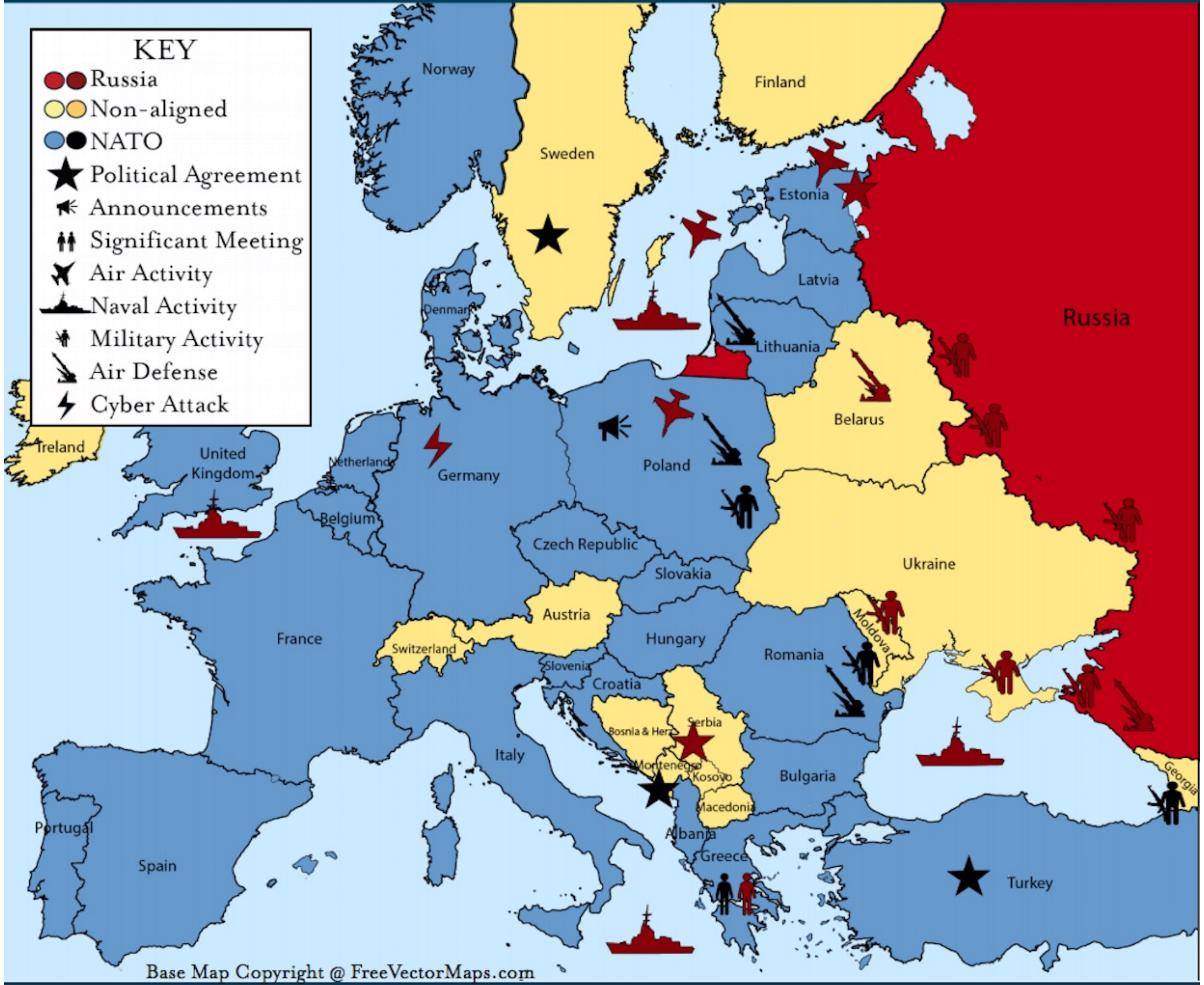
Foreign Intelligence Service of the Russian Federation (SVR)

- SVR are officially responsible for foreign intelligence operations it was formed from the 1st Directorate of the KGB which had been responsible for espionage
- The illegals made famous by the "Americans" were agents of SVR
- In 2010 the FBI arrested 10 agents of the SVR in the US. They were later released in a prisoner exchange with Russia.

Competition and the rise of the FSB (Galeotti 2017)

- These intelligence agencies rather then stick to their briefs compete for Putin’s attention.
- In Ukraine, for example, the SVR, FSB, and GRU, all ran competing operations.
- Since 2000 the FSB’s stature has risen while that of its competitors in Russian intelligence was falling.
- By the late 2000s, the GRU was in disgrace, due to its blunders in Russia’s 2008 war with Georgia, leading to abandoned airfields being bombed and Russian units getting outflanked.
- Putin also felt the SVR was too conservative and timid for limiting itself to simple information-gathering.

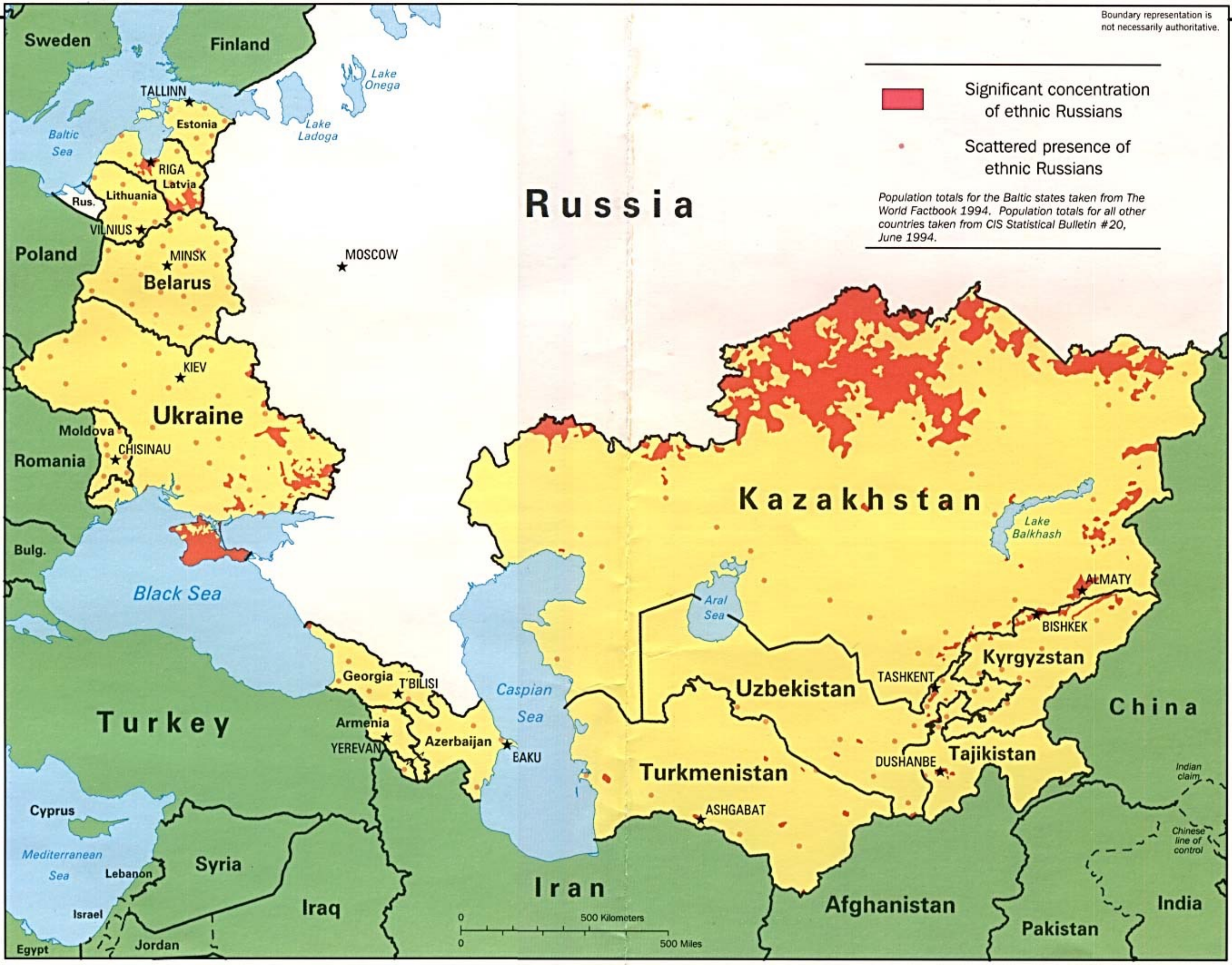
RUSSIA IN EUROPE: MAY 1–JUNE 14 2016



Base Map Copyright @ FreeVectorMaps.com

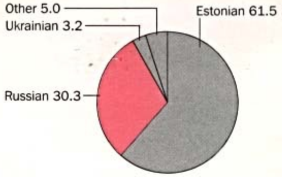
WWW.UNDERSTANDINGWAR.ORG

Ethnic Russians in the Newly Independent States



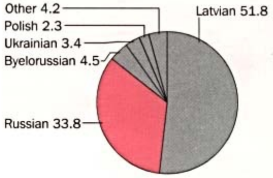
Population totals for the Baltic states taken from The World Factbook 1994. Population totals for all other countries taken from CIS Statistical Bulletin #20, June 1994.

Estonia
Percent



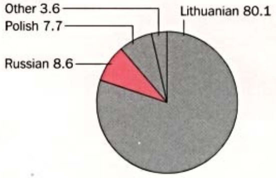
Population 1.6 million

Latvia
Percent



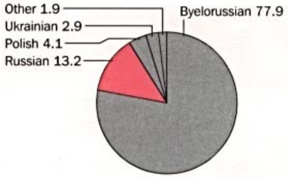
Population 2.7 million

Lithuania
Percent



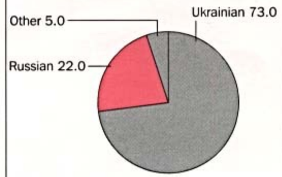
Population 3.8 million

Belarus
Percent



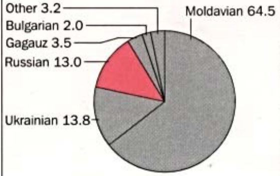
Population 10.4 million

Ukraine
Percent



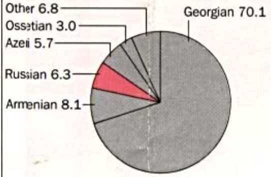
Population 52.1 million

Moldova
Percent



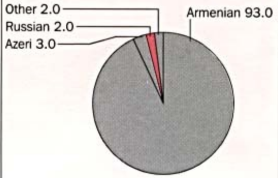
Population 4.4 million

Georgia*
Percent



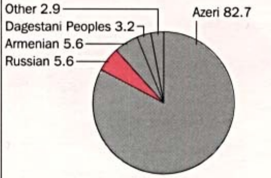
Population 5.4 million

Armenia*
Percent



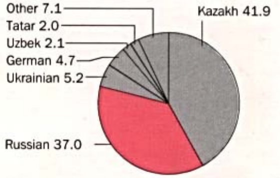
Population 3.7 million

Azerbaijan*
Percent



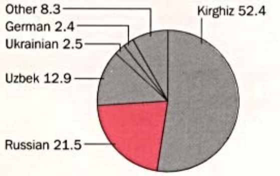
Population 7.4 million

Kazakhstan
Percent



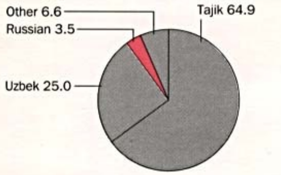
Population 16.9 million

Kyrgyzstan
Percent



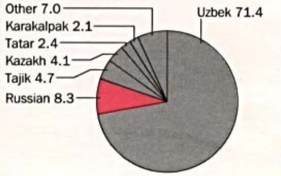
Population 4.5 million

Tajikistan
Percent



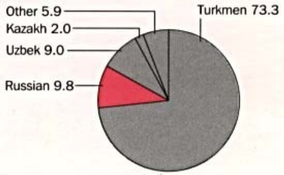
Population 5.7 million

Uzbekistan
Percent



Population 22.2 million

Turkmenistan
Percent



Population 4.4 million

*Ethnic percentages for Georgia, Armenia, and Azerbaijan taken from the 1989 Soviet census; they may not accurately reflect present-day conditions.

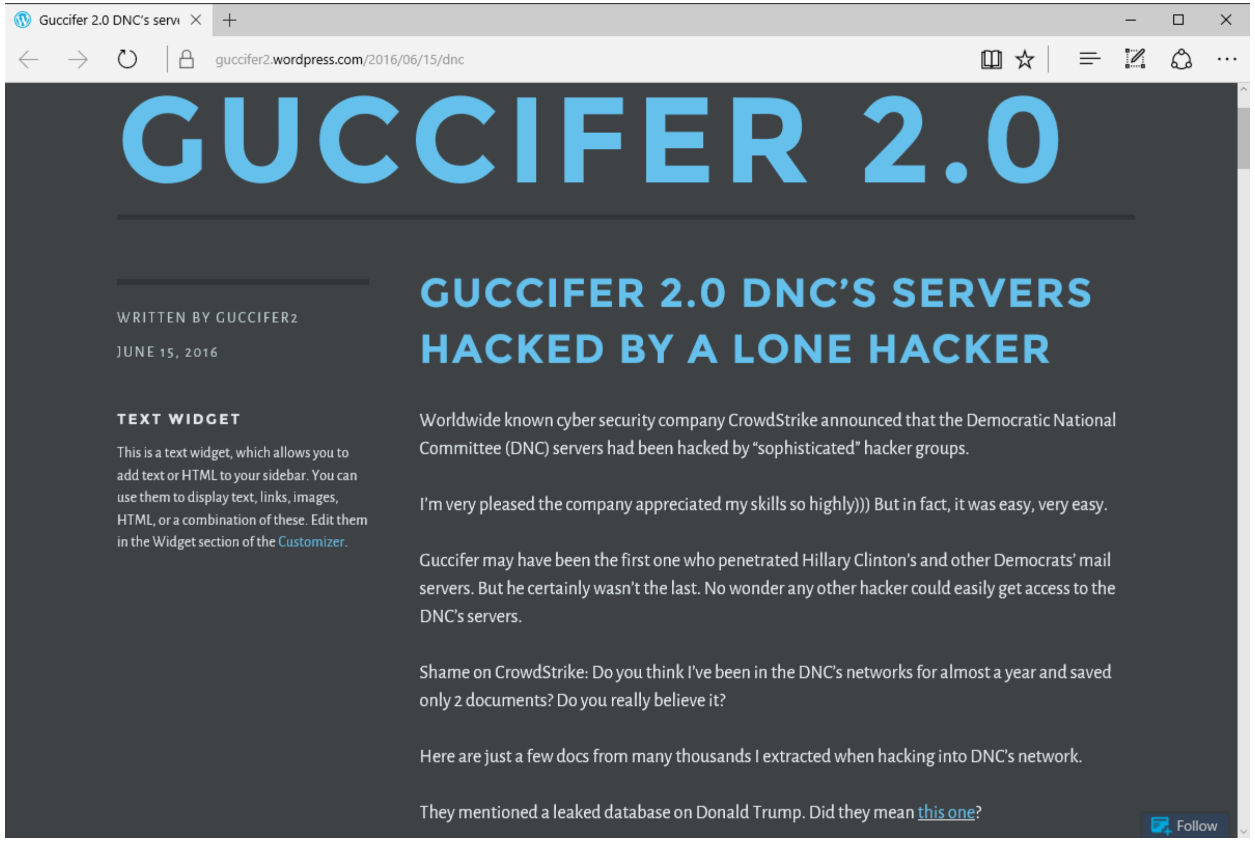
733683 (R01640) 10-94

Major Cyber Incidents in Eastern Europe

- Estonia 2007 - Large DDoS
- Georgia 2008 – Web defacement, suspected SCADA attacks
- Ukraine 2015 – IT/SCADA
- Ukraine 2016 - SCADA
- Ukraine 2017 – Destructive
- Ukraine 2022 – Dest/Infra/Satellite

Other Cyber Actions attributed to Russia

- Yahoo 2014-2016
- DNC hacks 2015-2016
- Other US Election Activity 2016
- Shadowbrokers 2016-2017
- French Election 2017
- Tainted Leaks 2017
- US Elections 2018/2020
- COVID Disinformation 2020
- Solarwinds 2021



GUCCIFER 2.0

WRITTEN BY GUCCIFER2

JUNE 15, 2016

TEXT WIDGET

This is a text widget, which allows you to add text or HTML to your sidebar. You can use them to display text, links, images, HTML, or a combination of these. Edit them in the Widget section of the Customizer.

GUCCIFER 2.0 DNC'S SERVERS HACKED BY A LONE HACKER

Worldwide known cyber security company CrowdStrike announced that the Democratic National Committee (DNC) servers had been hacked by "sophisticated" hacker groups.

I'm very pleased the company appreciated my skills so highly))) But in fact, it was easy, very easy.

Guccifer may have been the first one who penetrated Hillary Clinton's and other Democrats' mail servers. But he certainly wasn't the last. No wonder any other hacker could easily get access to the DNC's servers.

Shame on CrowdStrike: Do you think I've been in the DNC's networks for almost a year and saved only 2 documents? Do you really believe it?

Here are just a few docs from many thousands I extracted when hacking into DNC's network.

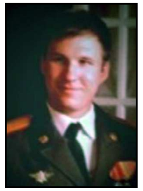
They mentioned a leaked database on Donald Trump. Did they mean this one?

Panoramic Visions Photography
Panoramicvisions.com

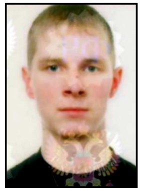
WANTED BY THE FBI

CONSPIRACY TO COMMIT AN OFFENSE AGAINST THE UNITED STATES; FALSE REGISTRATION OF A DOMAIN NAME; AGGRAVATED IDENTITY THEFT; CONSPIRACY TO COMMIT MONEY LAUNDERING

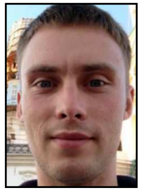
RUSSIAN INTERFERENCE IN 2016 U.S. ELECTIONS



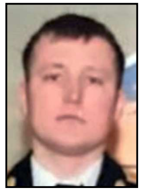
Boris Alekseyevich Antonov



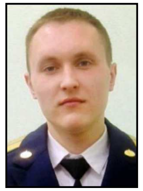
Dmitriy Sergeyevich Badin



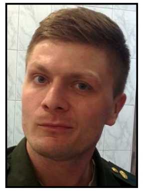
Anatoliy Sergeyevich Kovalev



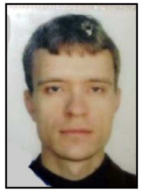
Nikolay Yuryevich Kozachek



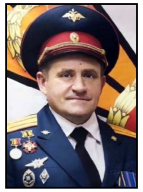
Aleksey Viktorovich Lukashev



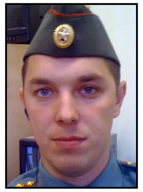
Artem Andreyevich Malyshev



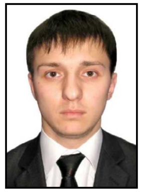
Sergey Aleksandrovich Morgachev



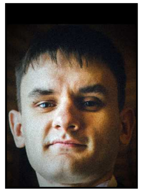
Aleksandr Vladimirovich Osadchuk



Aleksey Aleksandrovich Potemkin



Ivan Sergeyevich Yermakov



Pavel Vyacheslavovich Yershov

DETAILS

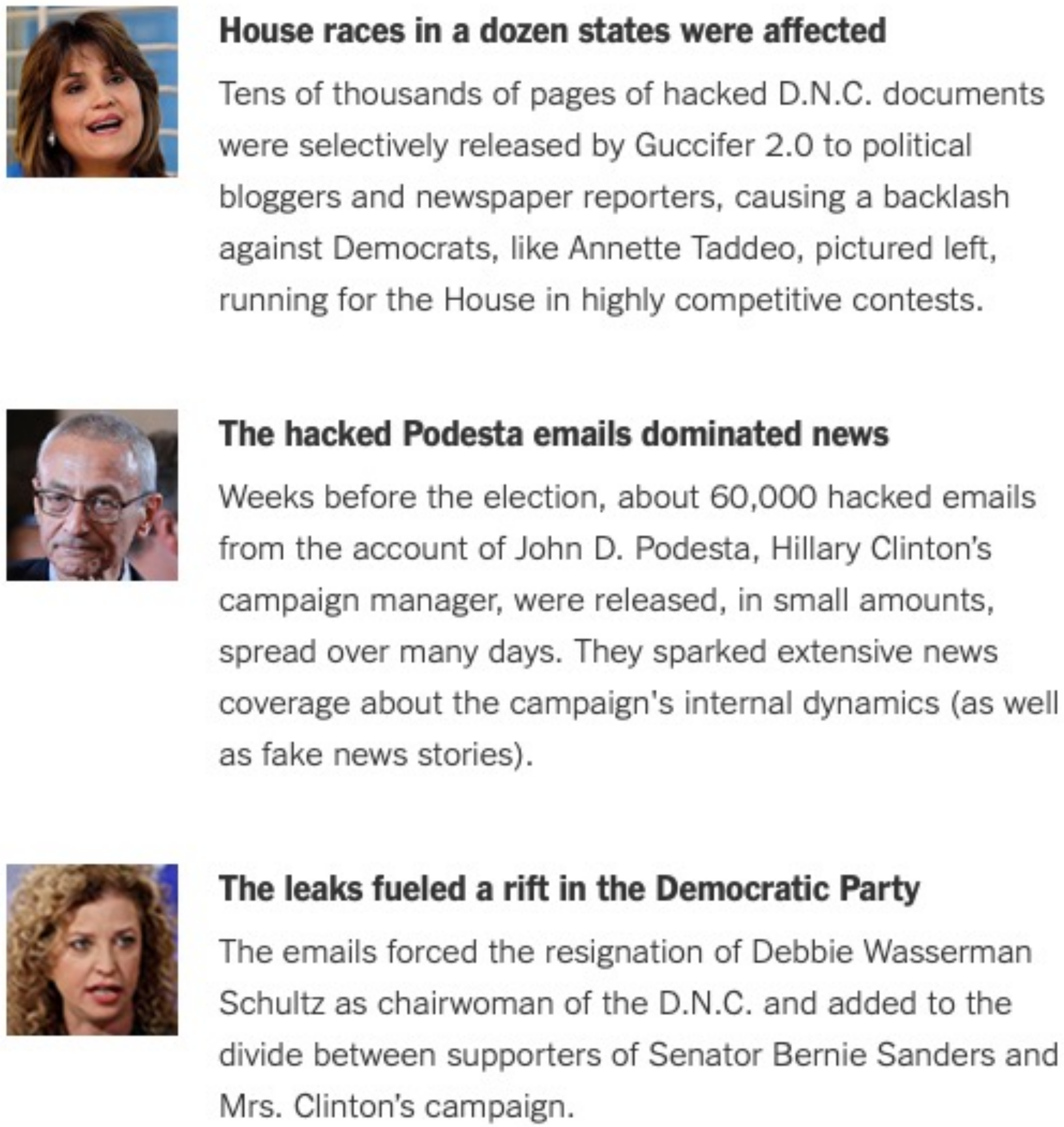
On July 13, 2018, a federal grand jury sitting in the District of Columbia returned an indictment against 12 Russian military intelligence officers for their alleged roles in interfering with the 2016 United States (U.S.) elections. The indictment charges 11 defendants, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Nikolay Yuryevich Kozachek, Aleksey Viktorovich Lukashev, Artem Andreyevich Malyshev, Sergey Aleksandrovich Morgachev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, Ivan Sergeyevich Yermakov, Pavel Vyacheslavovich Yershov, and Viktor Borisovich Netyksho, with a computer hacking conspiracy involving gaining unauthorized access into the computers of U.S. persons and entities involved in the 2016 U.S. presidential election, stealing documents from those computers, and staging releases of the stolen documents to interfere with the 2016 U.S. presidential election. The indictment also charges these defendants with aggravated identity theft, false registration of a domain name, and conspiracy to commit money laundering. Two defendants, Aleksandr Vladimirovich Osadchuk and Anatoliy Sergeyevich Kovalev, are charged with a separate conspiracy to commit computer crimes, relating to hacking into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections. The United States District Court for the District of Columbia in Washington, D.C. issued a federal arrest warrant for each of these defendants upon the grand jury's return of the indictment.

THESE INDIVIDUALS SHOULD BE CONSIDERED ARMED AND DANGEROUS, AN INTERNATIONAL FLIGHT RISK, AND AN ESCAPE RISK

If you have any information concerning this case, please contact your local FBI office, or the nearest American Embassy or Consulate.

www.fbi.gov

Results (New York Times)



House races in a dozen states were affected

Tens of thousands of pages of hacked D.N.C. documents were selectively released by Guccifer 2.0 to political bloggers and newspaper reporters, causing a backlash against Democrats, like Annette Taddeo, pictured left, running for the House in highly competitive contests.

The hacked Podesta emails dominated news

Weeks before the election, about 60,000 hacked emails from the account of John D. Podesta, Hillary Clinton's campaign manager, were released, in small amounts, spread over many days. They sparked extensive news coverage about the campaign's internal dynamics (as well as fake news stories).

The leaks fueled a rift in the Democratic Party

The emails forced the resignation of Debbie Wasserman Schultz as chairwoman of the D.N.C. and added to the divide between supporters of Senator Bernie Sanders and Mrs. Clinton's campaign.

(Source: Microsoft 2022)

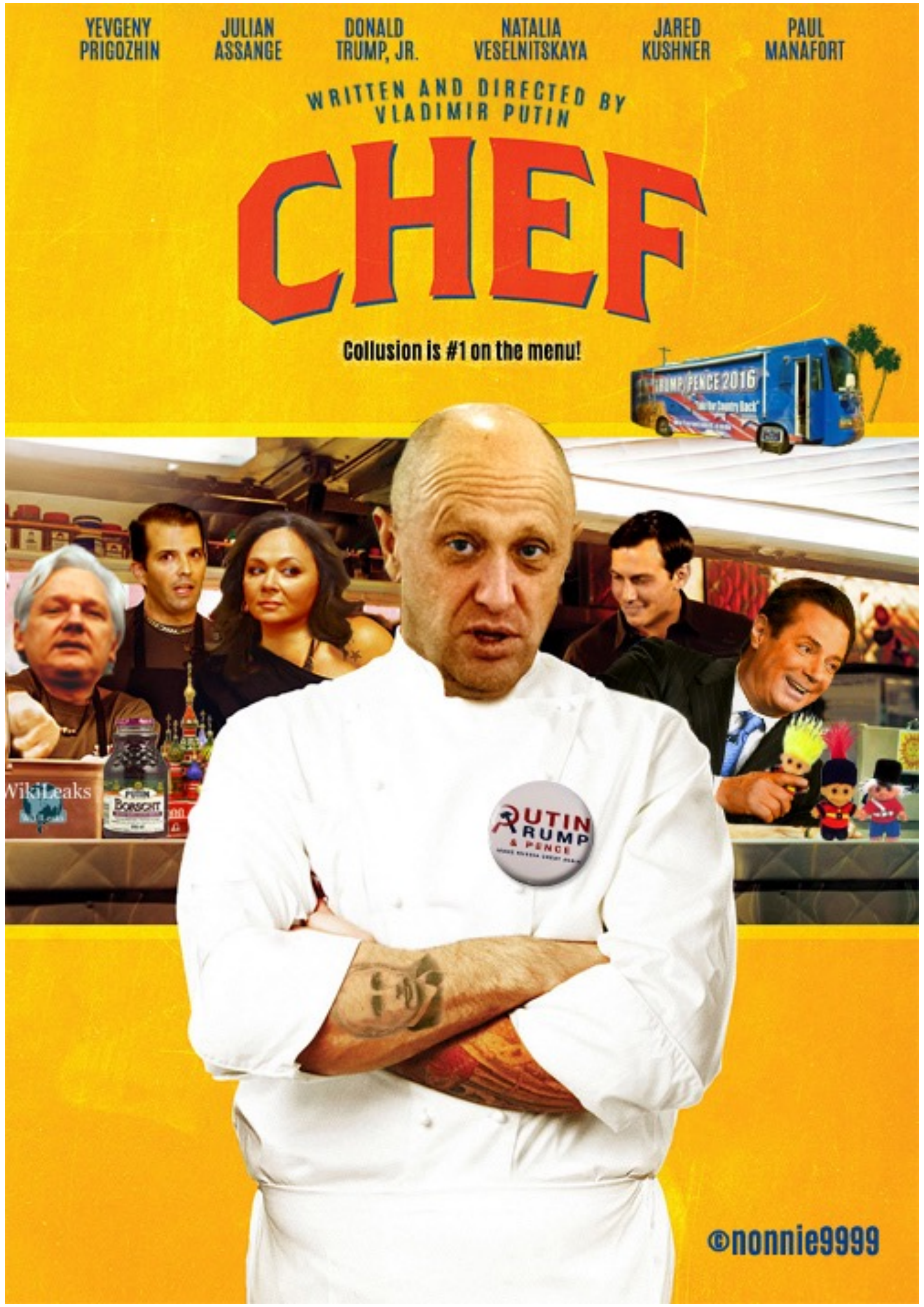
Bernie
2016
#SILENCED BY DNC
DNC 2016

State electoral authorities and vendors

- Quite separately from attacks on the DNC and Clinton campaign a number of state and local election entities were targeted by the GRU including state boards of election.
- In addition, vendors of voting software and hardware were also targeted.
- The GRU successfully accessed a database of all the registered voters in Illinois from that state's board of elections systems and exfiltrated many thousands of records (Mueller, 2019).

Internet Research Agency LLC

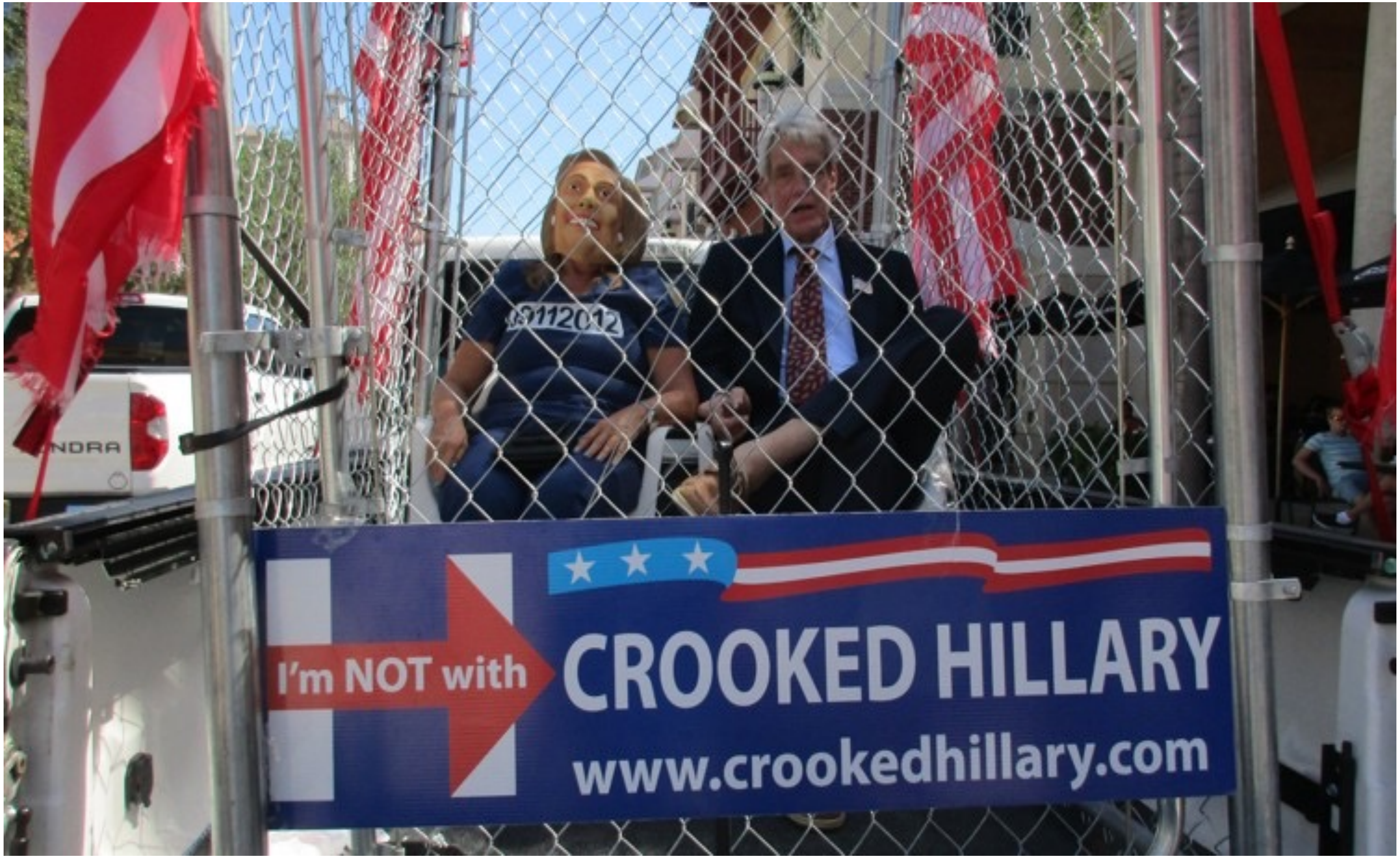
- In 2014 the IRA was established in St Petersburg, Russia (Smith, 2018). It has been estimated that the IRA employs over 400 people who occupy 40 rooms within its St Petersburg address.
- Discovered over the course of the US investigation, a memorandum instructs the defendants to focus on US politics using any opportunity to criticise Hillary and the other candidates, excluding Sanders and Trump.


YEVGENY PRIGOZHIN
JULIAN ASSANGE
DONALD TRUMP, JR.
NATALIA VESELNITSKAYA
JARED KUSHNER
PAUL MANAFORT
WRITTEN AND DIRECTED BY VLADIMIR PUTIN
CHEF
Collusion is #1 on the menu!
TRUMP PENCE 2016
WikiLeaks
PUTIN
BORSCHT
PUTIN RUMP & PENCE
©nonnie9999

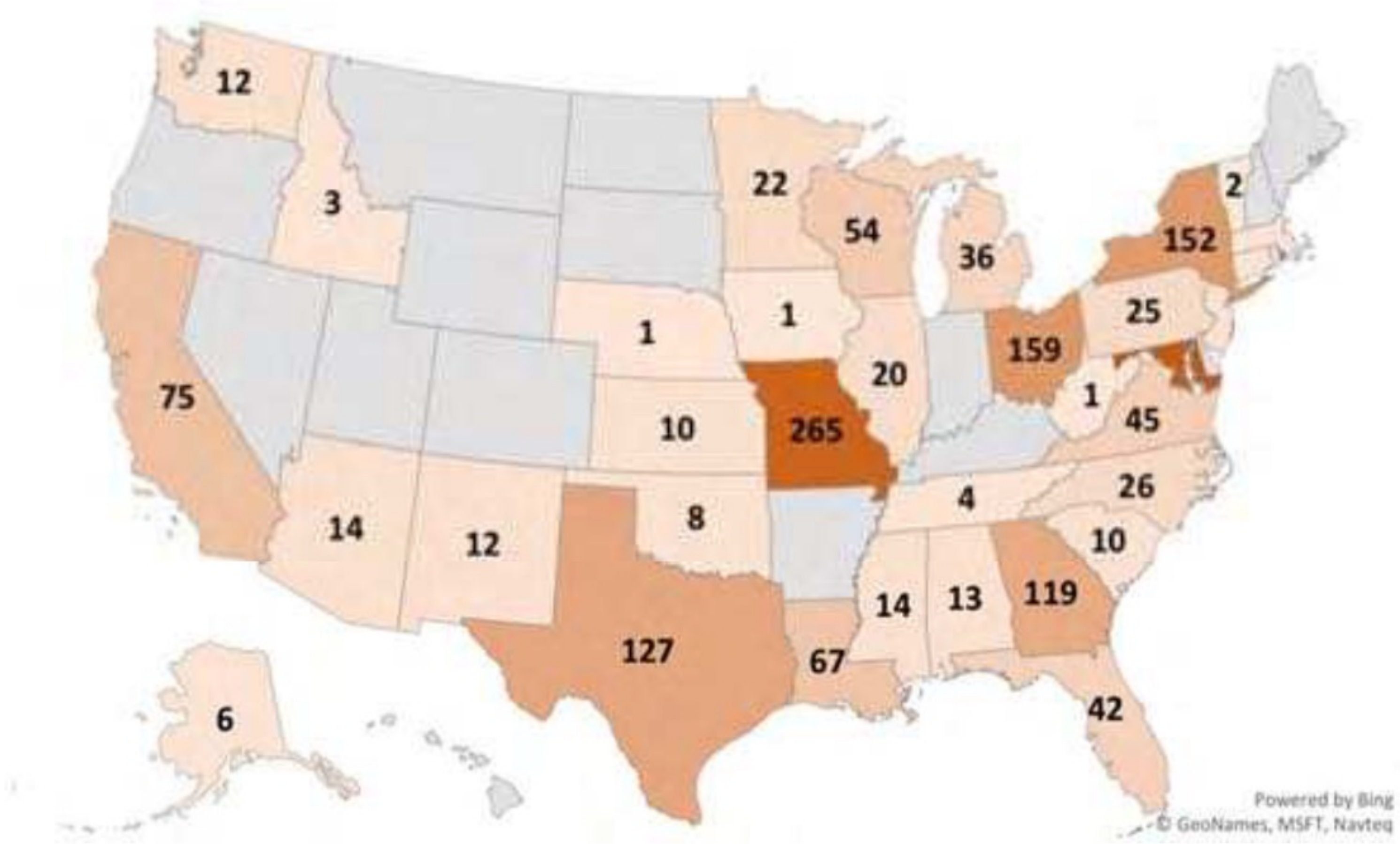
Events Organised by IRA

Event Date	Location	State	Theme
25/6/16	New York	New York	March for Trump
9/7/16	District of Columbia	District of Columbia	Support Hillary. Save American Muslims
23/7/16	New York	New York	Down with Hillary
20/8/16	West Palm Beach, Jupiter, Port St. Lucie, Miami, Hollywood, Fort Lauderdale and Coral Springs	Florida	Florida Goes for Trump
11/9/16	New York	New York	
11/9/16	Miami	Florida	
2/10/16	Various	Pennsylvannia	Miners for Trump

Florida Rally



Count of the number of times a state was targeted by IRA post (Howard et al., 2018)



Federal Agency of Government Communications and Information (FAPSI)

- FAPSI - Federal Agency of Government Communications and Information – was effectively Russia’s NSA
- The staff included graduates from the Orel Military Institute of Government Communications and the Institute of Cryptographic Communications of the FSB [Federal Security Service] Information Academy, as well as mathematicians, physicists, and electronics specialists.

FAPSI History

- In 1998 testimony to the United States Congress Joint Economic Committee by Victor Sheymov, a former KGB Major and head of the Cipher division, he observed a change in priorities for FAPSI with the end of the Cold War:
- *...the end of the Cold War somewhat shifted goals, objectives, and some targets of the FAPSI toward a heavier emphasis on intercept of technological, commercial and financial information. (Joint Economic Committee United States Congress 1998)*
- In 1996 FAPSI with its commercial arm created an Internet service provider called "Business Network of Russia" (Argentura 2007). While it is not known if it is linked to the notorious Russian Business Network

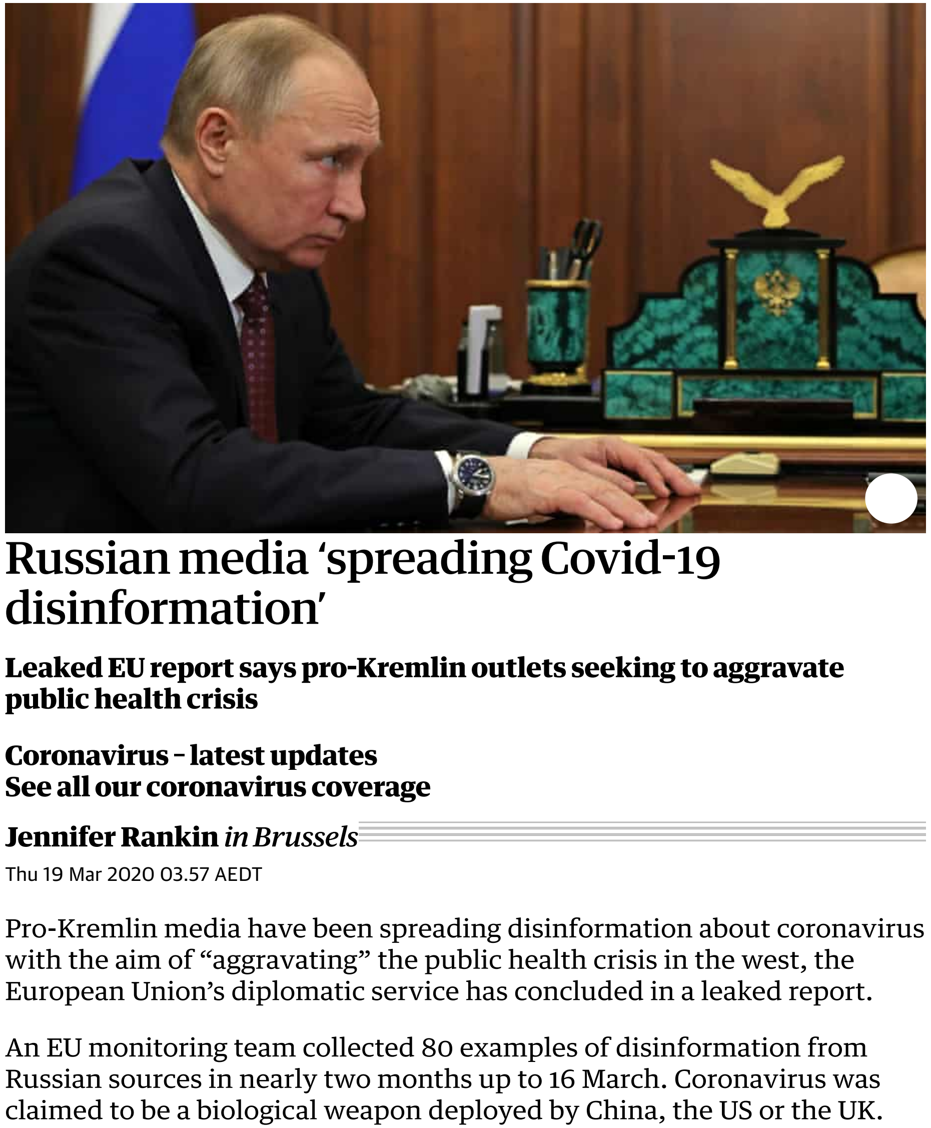
FAPSI and Organised Crime

- In 2003 FAPSI were disbanded
- Many former members of FAPSI were recruited by organised crime (Galeotti 2007)
- This is the same year phishing of Internet Banks became a problem
- Many of their FAPSI colleagues now work in the FSB and the GRU

CyberBerkut (Special Police)

- Group of Pro-Russian Activists
- Large Russia ethnic population in Ukraine
- Targeting Ukrainian Government and its supporters
- Proxy for FSB

COVID -19 Disinformation (Guardian)



Russian media 'spreading Covid-19 disinformation'

Leaked EU report says pro-Kremlin outlets seeking to aggravate public health crisis

Coronavirus – latest updates
See all our coronavirus coverage

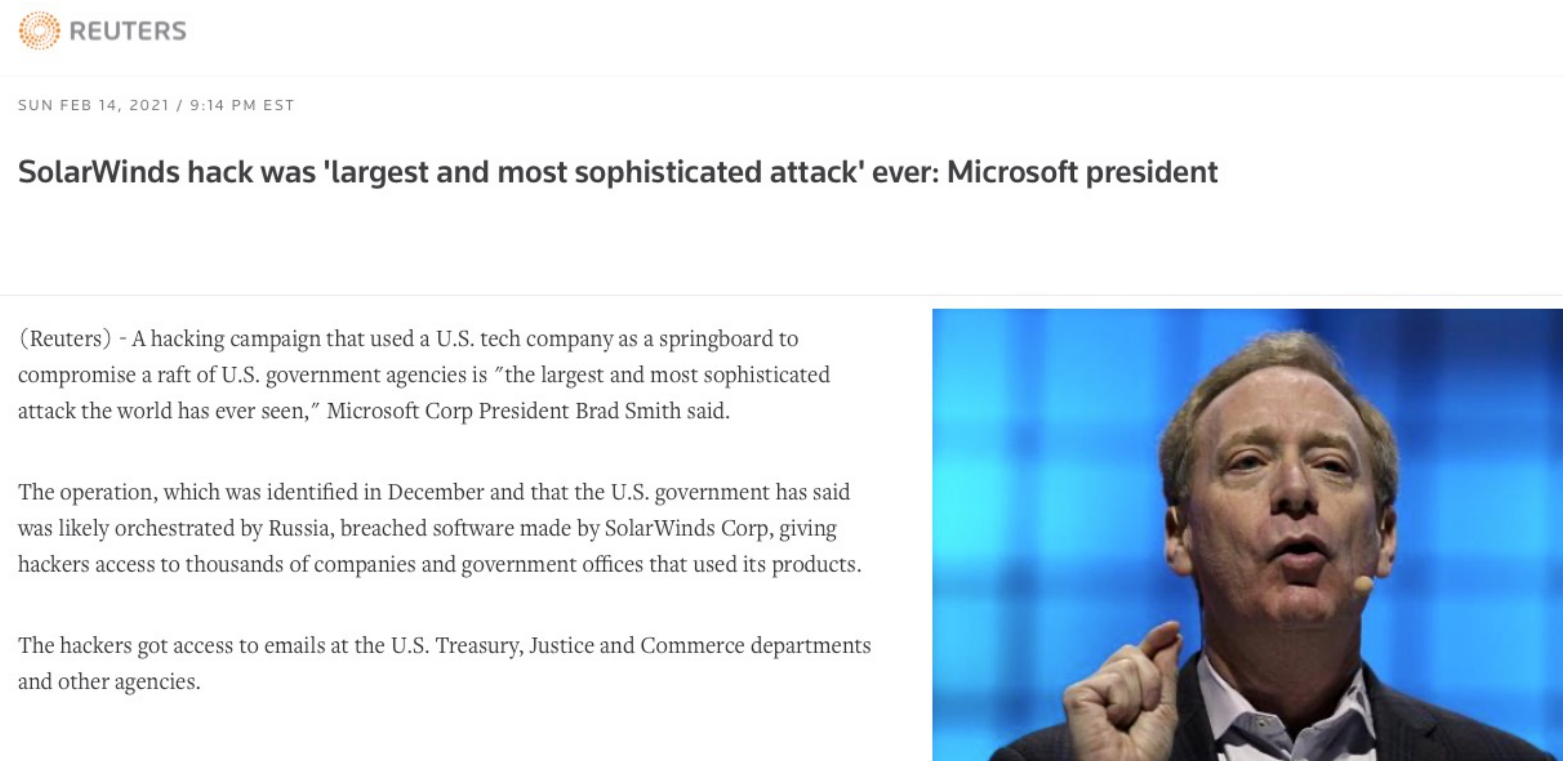
Jennifer Rankin *in Brussels*

Thu 19 Mar 2020 03.57 AEDT

Pro-Kremlin media have been spreading disinformation about coronavirus with the aim of "aggravating" the public health crisis in the west, the European Union's diplomatic service has concluded in a leaked report.

An EU monitoring team collected 80 examples of disinformation from Russian sources in nearly two months up to 16 March. Coronavirus was claimed to be a biological weapon deployed by China, the US or the UK.

SolarWinds (Reuters 2021)



REUTERS

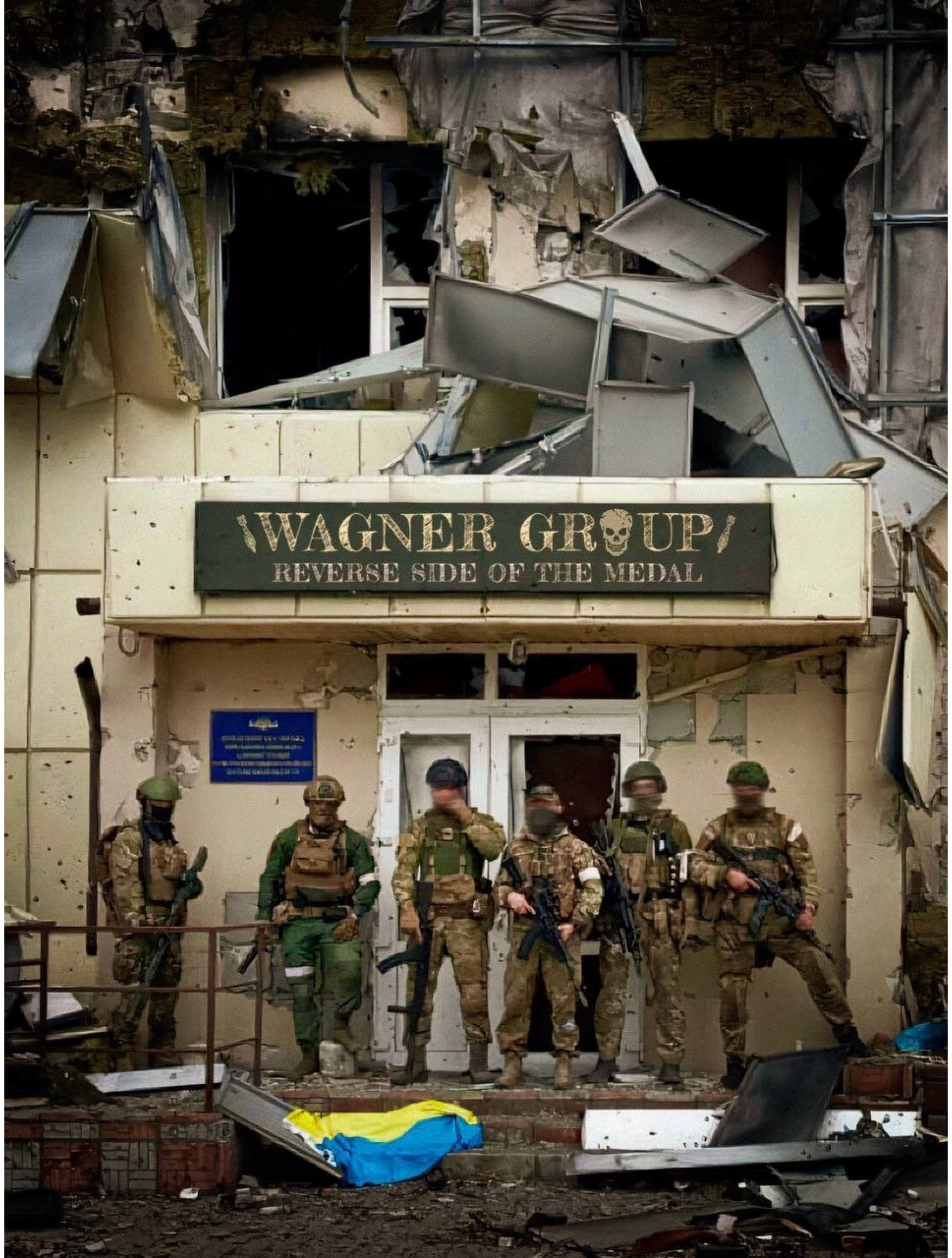
SUN FEB 14, 2021 / 9:14 PM EST

SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president

(Reuters) - A hacking campaign that used a U.S. tech company as a springboard to compromise a raft of U.S. government agencies is "the largest and most sophisticated attack the world has ever seen," Microsoft Corp President Brad Smith said.

The operation, which was identified in December and that the U.S. government has said was likely orchestrated by Russia, breached software made by SolarWinds Corp, giving hackers access to thousands of companies and government offices that used its products.

The hackers got access to emails at the U.S. Treasury, Justice and Commerce departments and other agencies.


WAGNER GROUP
REVERSE SIDE OF THE MEDAL

Wagner Group

The pre-history of modern Russian private military companies (PMCs)*

Tsarist Russia
The Tsarist Empire relied on the Cossacks to protect its borders and fight its wars, and assigned them various military tasks, including protecting the personal safety of the Russian tsar.

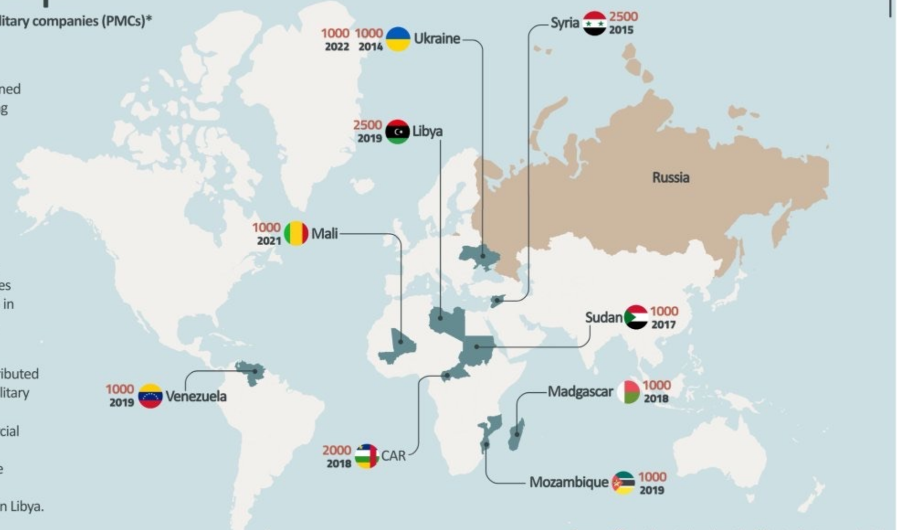
Civil War Period
Between 1917 and 1922, both parties employed paramilitary organizations and irregular militias and vigilante groups.

Soviet Empire
The Soviet Union sent military experts to train foreign irregular armed forces and regular forces of friendly countries. Sometimes, as happened in Libya, the trainers morphed into mercenaries.

Post-Cold War Collapse of the USSR
The sudden transition to the new system contributed to the weakening of the state's security and military apparatus. Many were employed in security companies protecting businesses and commercial and financial networks, some of which were suspicious and linked to organized crime. Some military experts and trainers remained in the countries in which they previously worked, as in Libya.

*Defence & Security Foresight Group (University of Waterloo)

Wagner Group's Global Footprint *



● Sources differ on the actual numbers; the highest estimates are adopted here, but many members of WG are now being redeployed in Ukraine.

*Radio Free Europe, Al Jazeera, BBC, DW, The Jerusalem Post, The Intercept

Wagner Group Roots

1 Volunteers who fought in various conflicts that arose within the former Soviet Union, including regions such as the Caucasus, Balkans, and parts of Central Asia.

2 Members of private armed forces that arose in the 1990s with the expansion of criminal networks. As the state centralized and tightened its grip on power, individuals moved to private security companies that provided services to influential people in the government, including President Putin.

3 Professional private military companies, most notably Moran Security Group, which fought on the side of the Syrian regime.

*Defence & Security Foresight Group (University of Waterloo)

About the group*

The number of Wagner contractors currently deployed in Africa is estimated at 10,000 mercenaries distributed in different countries.

The company is said to be registered in Argentina, but this seems difficult to officially confirm.

Wagner seeks to sign contracts with the governments of Ethiopia and Nigeria.

Until the summer of 2016, the training camp of the Wagner Group was located in Molkino, near Krasnodar in southern Russia, at the same location where a battalion of special forces and Russian military intelligence were stationed.

Al Jazeera, Fontanka, and Foreign Policy

Journalists Died Investigating Wagner*

April 2018

Maxim Borodin

An investigative journalist who revealed that Russian mercenaries working for a company called Wagner were killed in Syria. He died in mysterious circumstances after falling from the balcony of his apartment on the fifth floor in Yekaterinburg, Russia.

July 2018

Orkhan Dzhemal

Alexander Rastorguyev

Kirill Radchenko

Three Russian journalists who were investigating the activities of the Wagner Group in the Central African Republic. They were killed when the car they were traveling in was ambushed in Sibut, 200 km northeast of the capital Bangui.

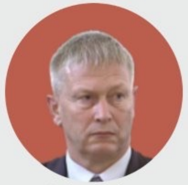
*BBC

THE SOUFAN CENTER

High-Profile Individuals Linked to Wagner Group*

Dmitriy Utkin

Founder and leader of the Wagner Group, which bears his call sign. Born in Ukraine, he participated in the Chechen wars and the 2014 Ukraine war and served in the Main Directorate of the General Staff of the Russian Armed Forces (Intelligence Directorate) until 2013. He worked with Moran Security Group and was part of the mission of the Slavonic Corps company to Syria. He was awarded the Order of Courage at an official ceremony held in the Kremlin, in which he appeared in a photo with President Putin.



Andrey Troshev

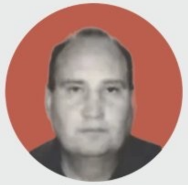
Retired colonel, founding member and "Chief of Staff" of the Wagner Group. A veteran of wars in Afghanistan and Chechnya, holder of the title of the Hero of the Russian Federation for his role in the first seizure of Palmyra, Syria in March 2016. He is subject to European sanctions for his role and participation in the group's military operations in Syria.

Andrei Bogatov

The commander of the fourth group specialized in reconnaissance and intelligence since 2014. He lost his arm by friendly fire in the battle of Palmyra, and then headed a team protecting critical infrastructure, including an oil refinery. He is subject to European sanctions for his role and participation in the group's military operations in Syria.

Alexander Kuznetsov

Nickname Ratibor. Commander of an assault squadron in the Wagner Group. He was a Major in the Special Forces before he was imprisoned in 2008 for kidnapping and burglary. In 2014, he joined the Wagner Group and fought in its ranks in Ukraine and Syria. He was wounded in Libya while fighting alongside Haftar's forces, and the European Union accuses him of "threatening peace, security and stability" in Libya.



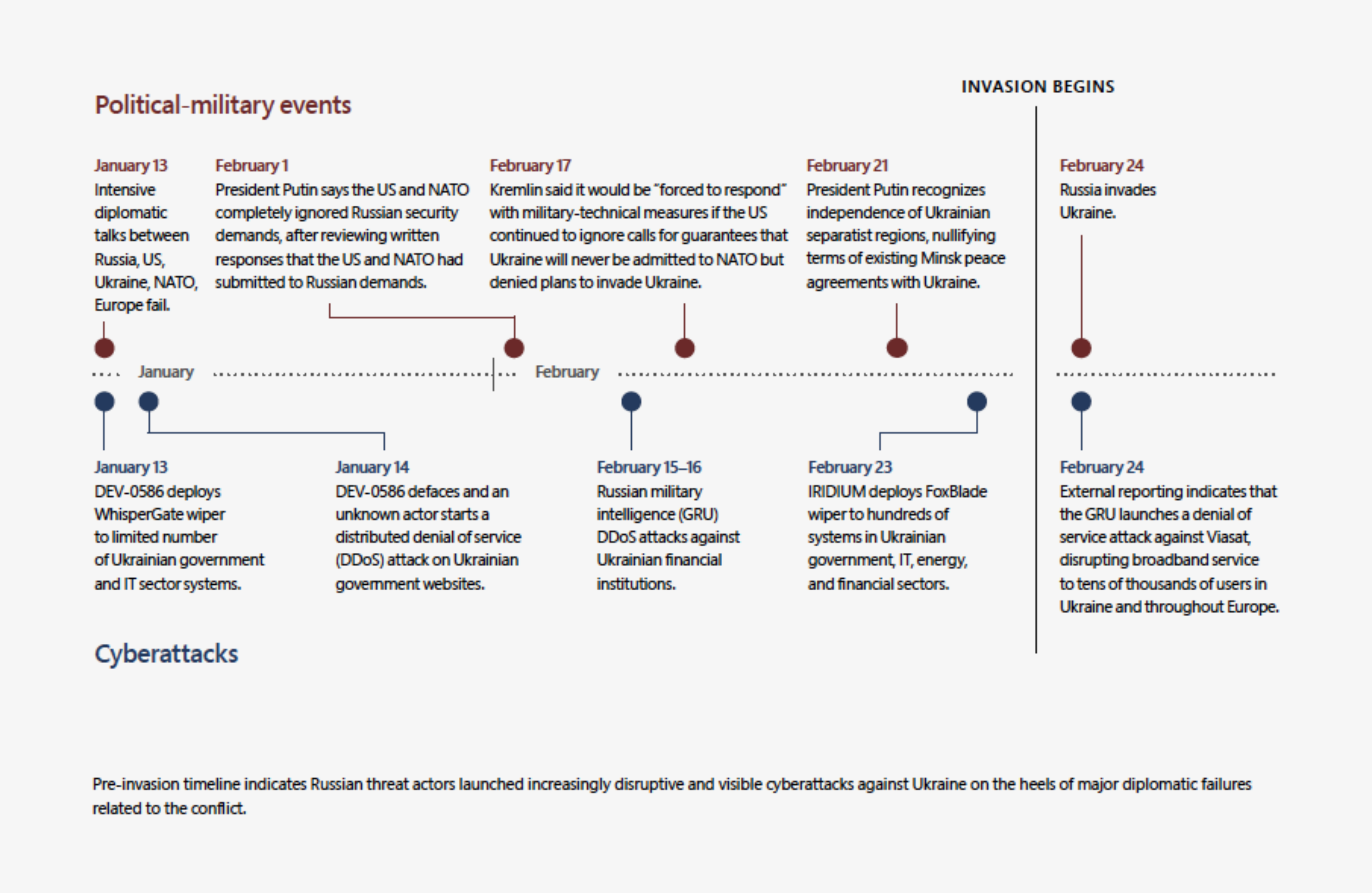
Valery Zakharov

Security Adviser to the President of the Central African Republic. The European Union accuses him of orchestrating the murder of three Russian reporters in the Central African Republic and describes him as a key figure in the Wagner Group command structure.

Yevgeny Prigozhin

Wagner Group financier. A businessman who made his fortune in the 1990s from his catering business. Closely associated with President Vladimir Putin and nicknamed "Putin's Chef" as his company caters to the official banquets of the Kremlin and Russian President Putin. He is subject to US sanctions for interfering in the 2016 US presidential campaign. He was imprisoned in 1981 for theft and fraud, and spent 9 years in prison.

*Respublika - Center for Civil Resistance, The Guardian, Al Jazeera, Reuters, Fontanka, The Times



INVASION BEGINS

Political-military events

January 13
Intensive diplomatic talks between Russia, US, Ukraine, NATO, Europe fail.

February 1
President Putin says the US and NATO completely ignored Russian security demands, after reviewing written responses that the US and NATO had submitted to Russian demands.

February 17
Kremlin said it would be "forced to respond" with military-technical measures if the US continued to ignore calls for guarantees that Ukraine will never be admitted to NATO but denied plans to invade Ukraine.

February 21
President Putin recognizes independence of Ukrainian separatist regions, nullifying terms of existing Minsk peace agreements with Ukraine.

February 24
Russia invades Ukraine.

January 13
DEV-0586 deploys WhisperGate wiper to limited number of Ukrainian government and IT sector systems.

January 14
DEV-0586 defaces and an unknown actor starts a distributed denial of service (DDoS) attack on Ukrainian government websites.

February 15–16
Russian military intelligence (GRU) DDoS attacks against Ukrainian financial institutions.

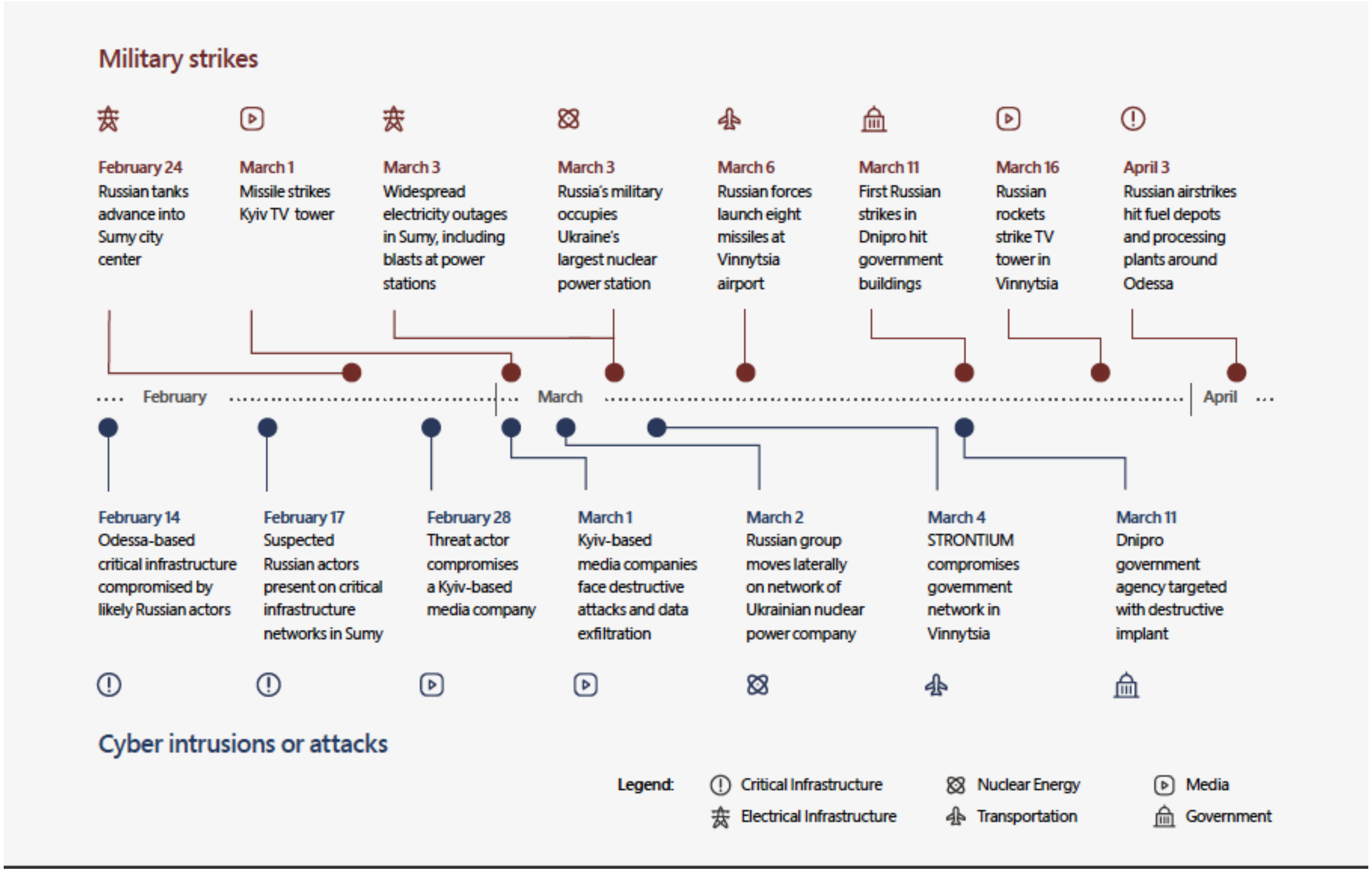
February 23
IRIDIUM deploys FoxBlade wiper to hundreds of systems in Ukrainian government, IT, energy, and financial sectors.

February 24
External reporting indicates that the GRU launches a denial of service attack against Viasat, disrupting broadband service to tens of thousands of users in Ukraine and throughout Europe.

Cyberattacks

Pre-invasion timeline indicates Russian threat actors launched increasingly disruptive and visible cyberattacks against Ukraine on the heels of major diplomatic failures related to the conflict.

(Source: Microsoft 2022)



Military strikes

February 24
Russian tanks advance into Sumy city center

March 1
Missile strikes Kyiv TV tower

March 3
Widespread electricity outages in Sumy, including blasts at power stations

March 3
Russia's military occupies Ukraine's largest nuclear power station

March 6
Russian forces launch eight missiles at Vinnytsia airport

March 11
First Russian strikes in Dnipro hit government buildings

March 16
Russian rockets strike TV tower in Vinnytsia

April 3
Russian airstrikes hit fuel depots and processing plants around Odessa

February 14
Odessa-based critical infrastructure compromised by likely Russian actors

February 17
Suspected Russian actors present on critical infrastructure networks in Sumy

February 28
Threat actor compromises a Kyiv-based media company

March 1
Kyiv-based media companies face destructive attacks and data exfiltration

March 2
Russian group moves laterally on network of Ukrainian nuclear power company

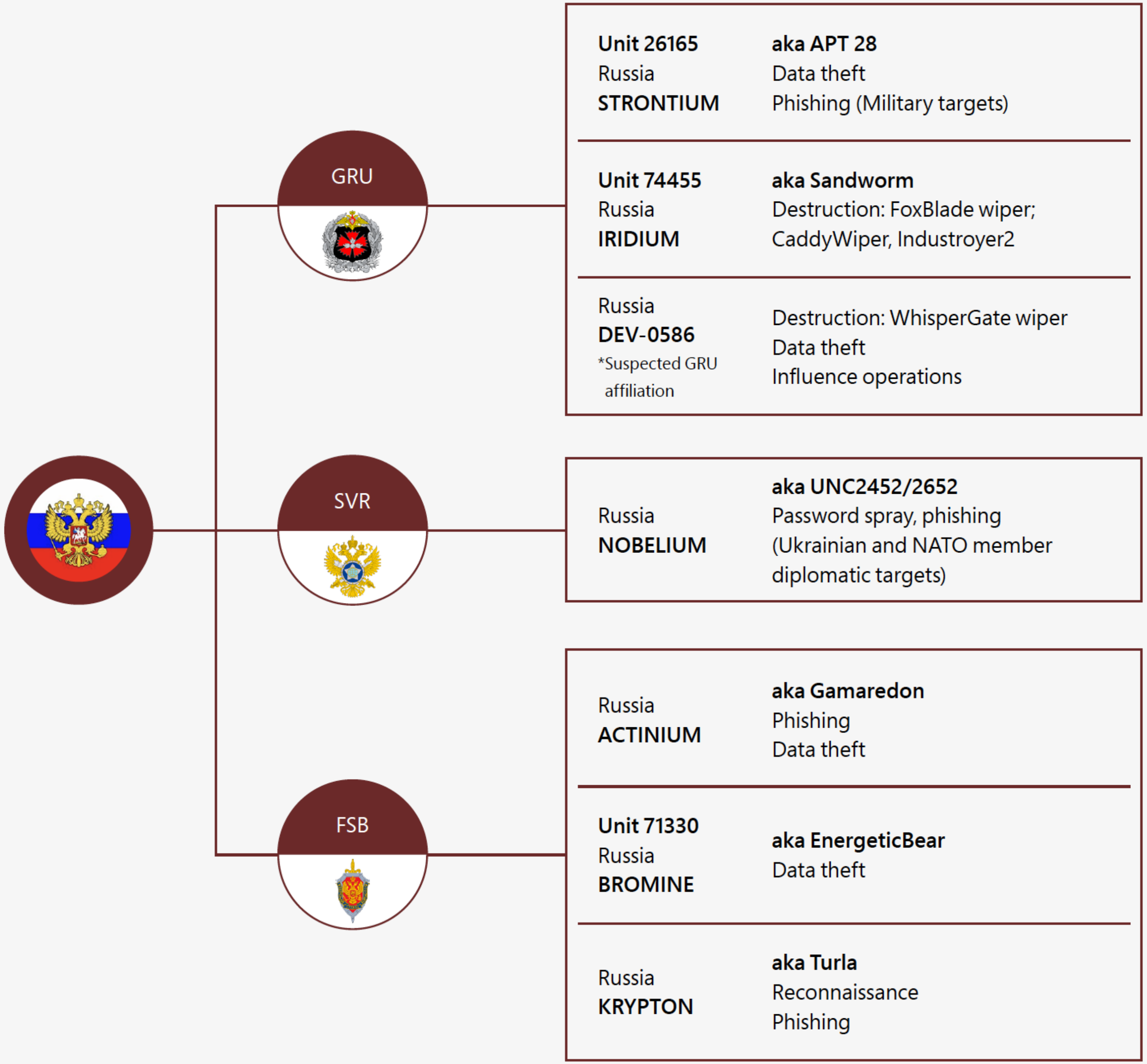
March 4
STRONTIUM compromises government network in Vinnytsia

March 11
Dnipro government agency targeted with destructive implant

Cyber intrusions or attacks

Legend: Critical Infrastructure; Electrical Infrastructure; Nuclear Energy; Transportation; Media; Government

(Source: Microsoft 2022)



GRU

Unit 26165
Russia
STRONTIUM

aka APT 28
Data theft
Phishing (Military targets)

Unit 74455
Russia
IRIDIUM

aka Sandworm
Destruction: FoxBlade wiper; CaddyWiper, Industroyer2

Russia
DEV-0586
*Suspected GRU affiliation

Destruction: WhisperGate wiper
Data theft
Influence operations

SVR

Russia
NOBELIUM

aka UNC2452/2652
Password spray, phishing (Ukrainian and NATO member diplomatic targets)

FSB

Russia
ACTINIUM

aka Gamaredon
Phishing
Data theft

Unit 71330
Russia
BROMINE

aka EnergeticBear
Data theft

Russia
KRYPTON

aka Turla
Reconnaissance
Phishing

(Source: Microsoft 2022)

China - Three Warfares

- Work Guidelines of the People's Liberation Army commonly known as China's Three Warfares — which are:
    - public opinion warfare,
    - psychological warfare,
    - and legal warfare.

China IP Theft

- Chinese cyber IP theft is consistent with its government policies of technology transfer
- “Chinese companies have been pillaging the intellectual property of American companies. All together, intellectual-property theft costs America up to $600 billion a year, the greatest transfer of wealth in history. China accounts for most of that loss Intellectual-property theft covers a wide spectrum: counterfeiting American fashion designs, pirating movies and video games, patent infringement and stealing proprietary technology and software. (NYT Blair & Alexander 2017)”
- “Bolstered by its commercial heft, China’s global ambition is increasingly built on ports, highways and pipelines in the expansion of its supply chain empire. More than this, China's grand strategy is built on developing new markets for advanced Chinese technology (Forbes Araya 2019).”

China

- China’s capability includes the Ministry of State Security which is responsible for overseas intelligence and keeping an eye on troublesome minority groups within China.
- The Chinese military, the People Liberation Army (PLA), have large information warfare units which while largely defensive also have offensive capabilities and are used for info war including espionage.

Origins of Chinese Cyber Capability

- In 1990s Chinese military thinking observed the importance of targeting IT systems in US attacks and First Gulf war in 1990-91 on Yugoslavia in 1999
- Downing of Chinese Jet over Hainan in 2000 showed role of patriotic hackers with Code Red
- Titan Rain (Byzantine Hades) attacks in 2004/2005 against US military networks showed their cyber military capability
- 2010 PLA Daily announced the establishment of formal PLA cyber command
- In 2016 PLA Strategic Support Force was formed for cyber warfare, space warfare, and electronic warfare

PLASSF Commander (Adam Ni)

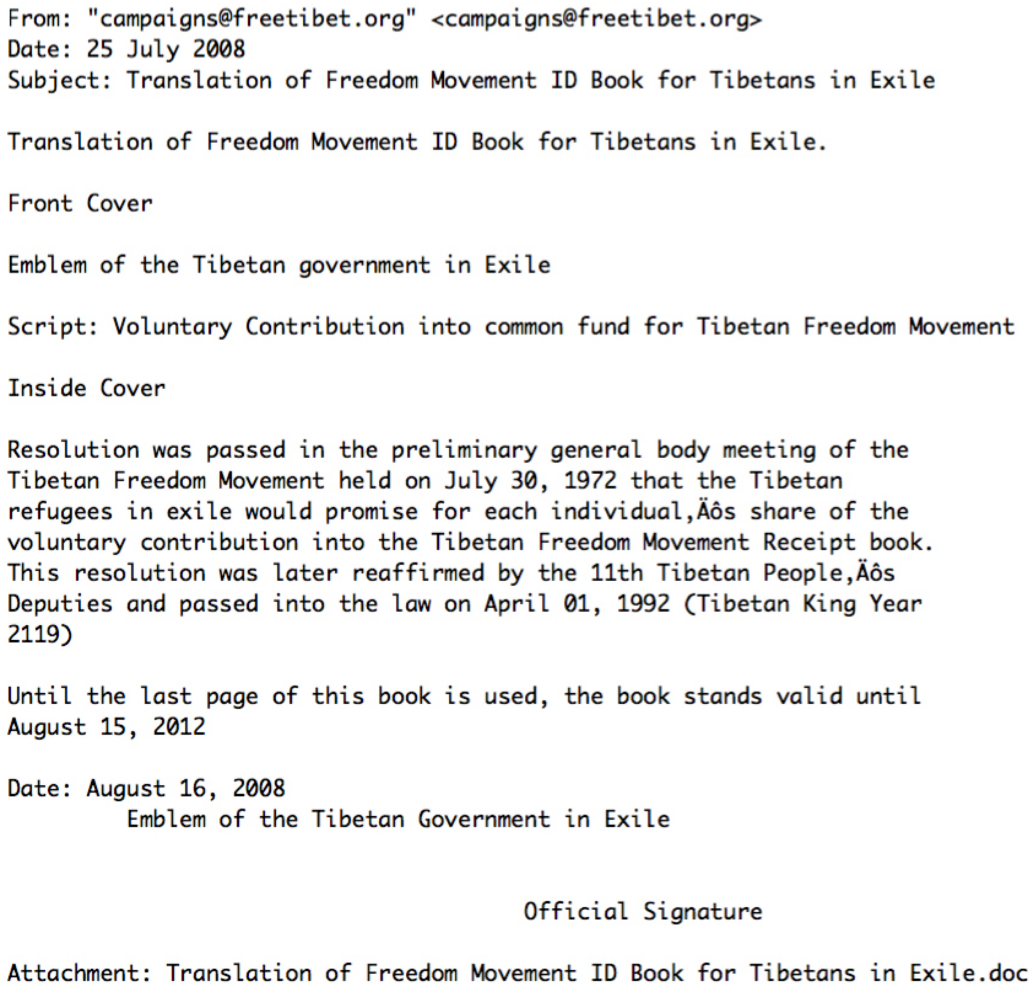
Counter- Intelligence Trinity (Lam 2018)

- Employ new laws and regulations to integrate national counterintelligence efforts, as
- Improve communication between Chinese security agencies, civilian and military, and
- Advance a “broad concept of national security” going beyond traditional counterintelligence from earlier, less connected times to better protect China in a time of heightened foreign influence inside the PRC

China and Australian Mining

- Australian Mining Sector including Rio Tinto Group, BHP Billiton Ltd. and Fortescue Metal Groups have been targeted by Chinese state sponsored attacks dating back to 2008.
- PLA units were seeking intelligence on pricing to assist in negotiations.
- Head of UK’s MI5 said Rio Tinto attack cost over AUD$1 Billion
- The theft of intellectual property such as production methods, mineral processing methods, chemical formulae, custom software also targeted by state sponsored groups to assisting their own industries to compete.

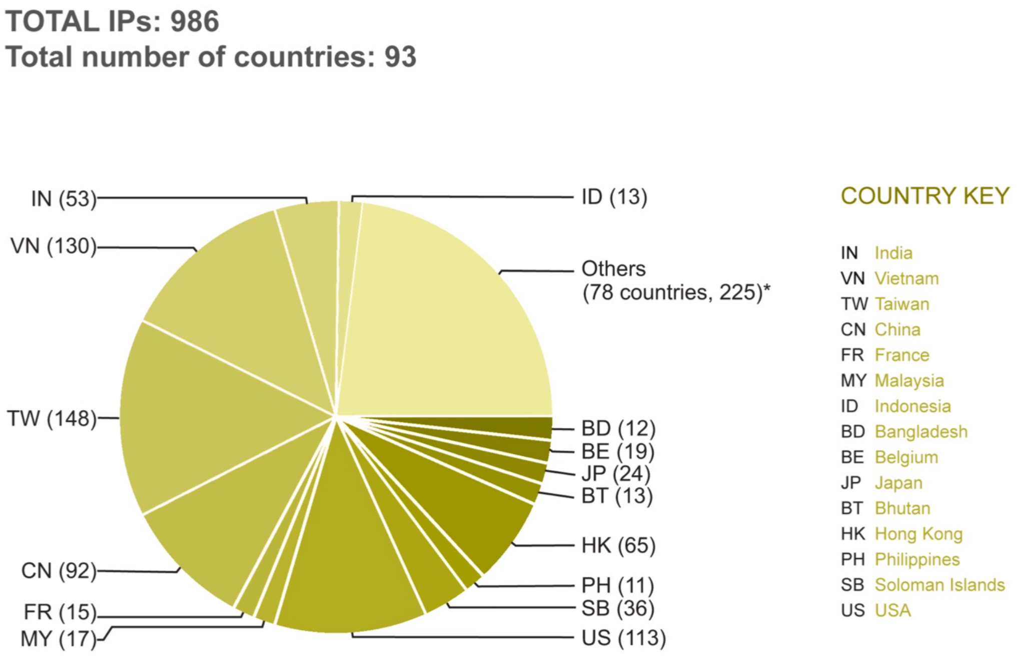
Tibetan Activists Targeted (Citizen Lab 2009)



```
From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the
Tibetan Freedom Movement held on July 30, 1972 that the Tibetan
refugees in exile would promise for each individual,Äôs share of the
voluntary contribution into the Tibetan Freedom Movement Receipt book.
This resolution was later reaffirmed by the 11th Tibetan People,Äôs
Deputies and passed into the law on April 01, 1992 (Tibetan King Year
2119)

Until the last page of this book is used, the book stands valid until
August 15, 2012

Date: August 16, 2008
         Emblem of the Tibetan Government in Exile


                                       Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc
```

GhostNet Infection Distribution (Information Warfare Monitor 2009)

Fig. 12
The geographic location of infected hosts.



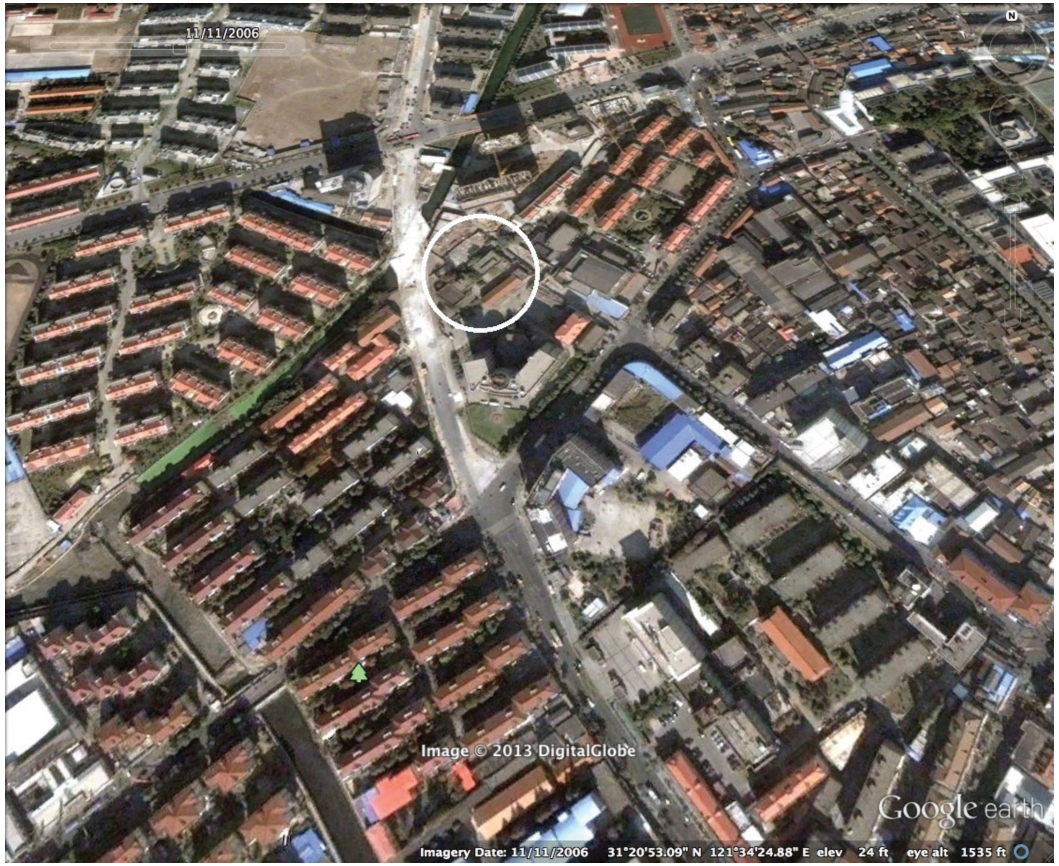
COUNTRY KEY

IN	India
VN	Vietnam
TW	Taiwan
CN	China
FR	France
MY	Malaysia
ID	Indonesia
BD	Bangladesh
BE	Belgium
JP	Japan
BT	Bhutan
HK	Hong Kong
PH	Philippines
SB	Soloman Islands
US	USA

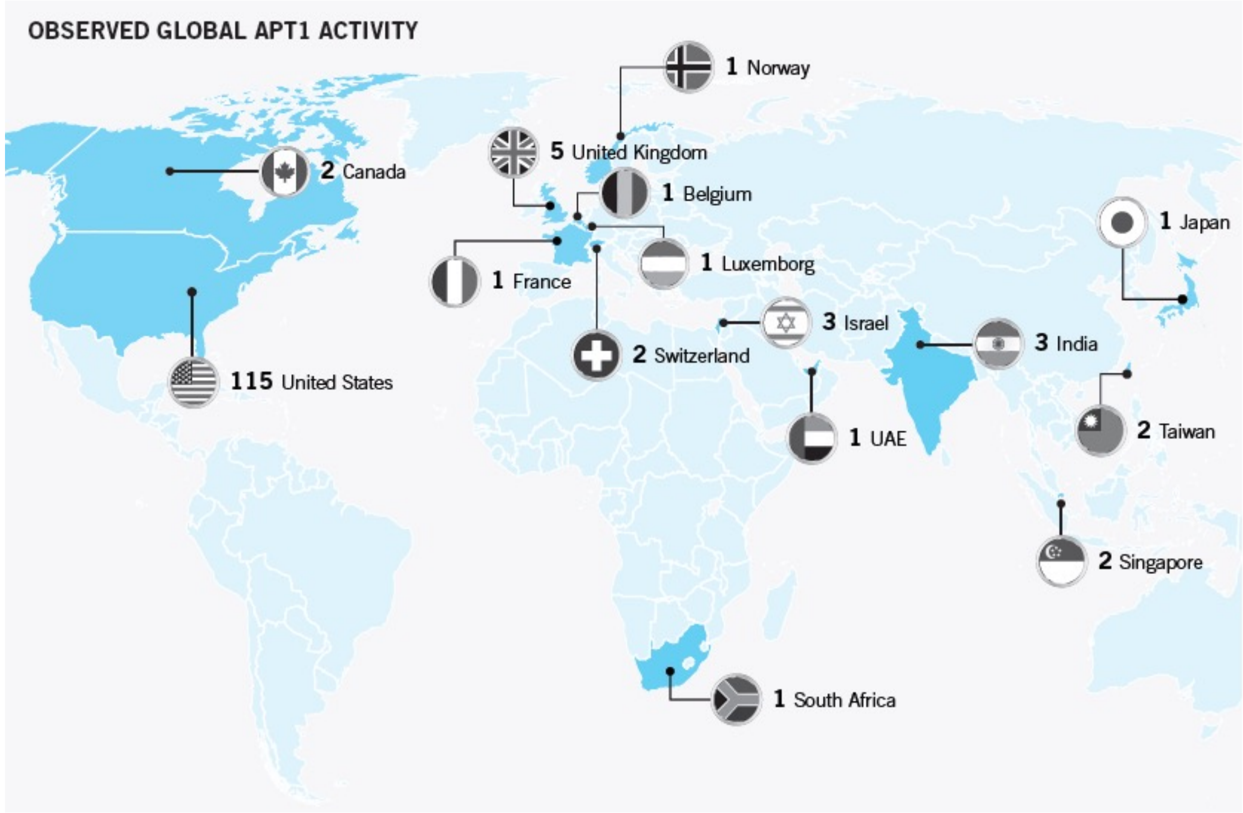
APT 1 (Mandiant 2013)

- Mandiant’s analysis has led them conclude that APT1 is likely government-sponsored and one of the most persistent of China’s cyber threat actors.
- In seeking to identify the organization behind this activity, their research found that People’s Liberation Army (PLA’s) Unit 61398 is similar to APT1 in its mission, capabilities, and resources.

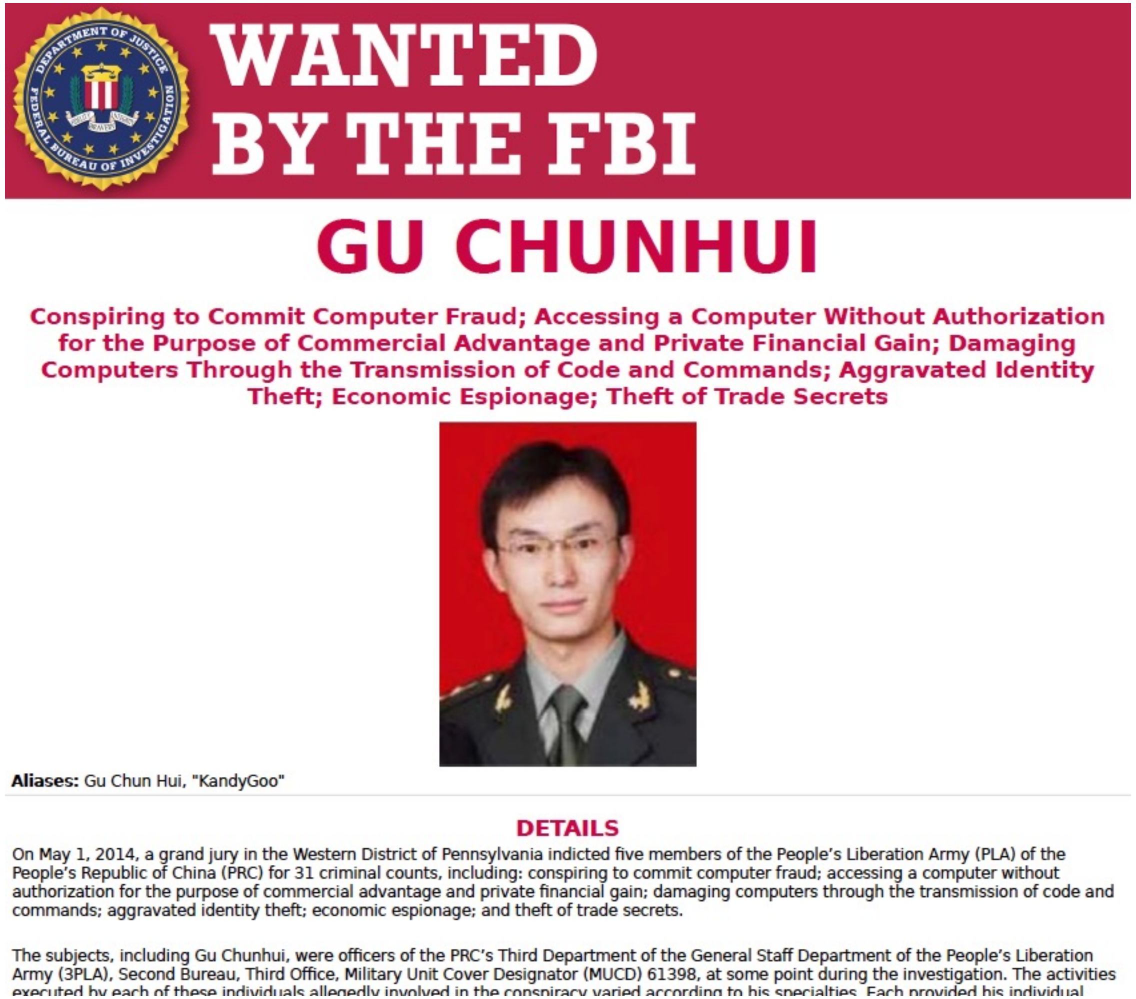
APT 1 (Mandiant)


11/11/2006
Image © 2013 DigitalGlobe
Google earth
Imagery Date: 11/11/2006 31°20'53.09" N 121°34'24.88" E elev 24 ft eye alt 1535 ft

APT 1 (Mandiant)



PLA Indictments (DOJ 2014)



WANTED BY THE FBI

GU CHUNHUI

Conspiring to Commit Computer Fraud; Accessing a Computer Without Authorization for the Purpose of Commercial Advantage and Private Financial Gain; Damaging Computers Through the Transmission of Code and Commands; Aggravated Identity Theft; Economic Espionage; Theft of Trade Secrets

Aliases: Gu Chun Hui, "KandyGoo"

DETAILS

On May 1, 2014, a grand jury in the Western District of Pennsylvania indicted five members of the People's Liberation Army (PLA) of the People's Republic of China (PRC) for 31 criminal counts, including: conspiring to commit computer fraud; accessing a computer without authorization for the purpose of commercial advantage and private financial gain; damaging computers through the transmission of code and commands; aggravated identity theft; economic espionage; and theft of trade secrets.

The subjects, including Gu Chunhui, were officers of the PRC's Third Department of the General Staff Department of the People's Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398, at some point during the investigation. The activities executed by each of these individuals allegedly involved in the conspiracy varied according to his specialties. Each provided his individual

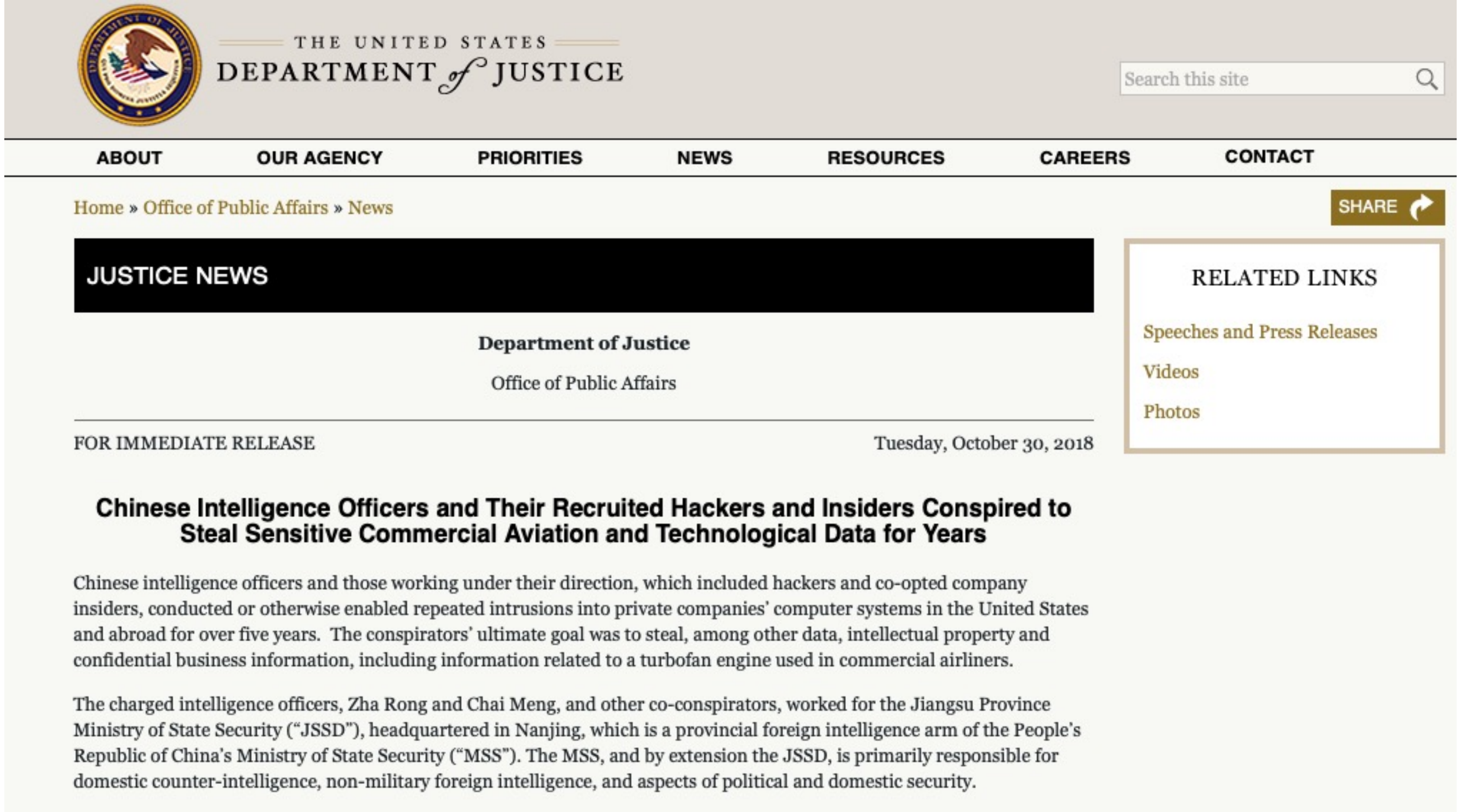
Putter Panda (Crowdstrike 2014)

- Putter Panda is a cyber espionage actor that conducts operations from Shanghai, China, likely on behalf of the Chinese People’s Liberation Army (PLA) 3rd General Staff Department 12th Bureau Unit 61486.
- This unit is supports the space based signals intelligence (SIGINT) mission.

Chen Ping, aka cpyy

- The attribution provided in this report points to Chen Ping, aka cpyy (born on May 29, 1979), as an individual responsible for the domain registration for the Command and Control (C2) of PUTTER PANDA malware.

MSS Indictments (DOJ 2018)


THE UNITED STATES DEPARTMENT of JUSTICE
Search this site
ABOUT
OUR AGENCY
PRIORITIES
NEWS
RESOURCES
CAREERS
CONTACT
Home » Office of Public Affairs » News
SHARE
RELATED LINKS
Speeches and Press Releases
Videos
Photos

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

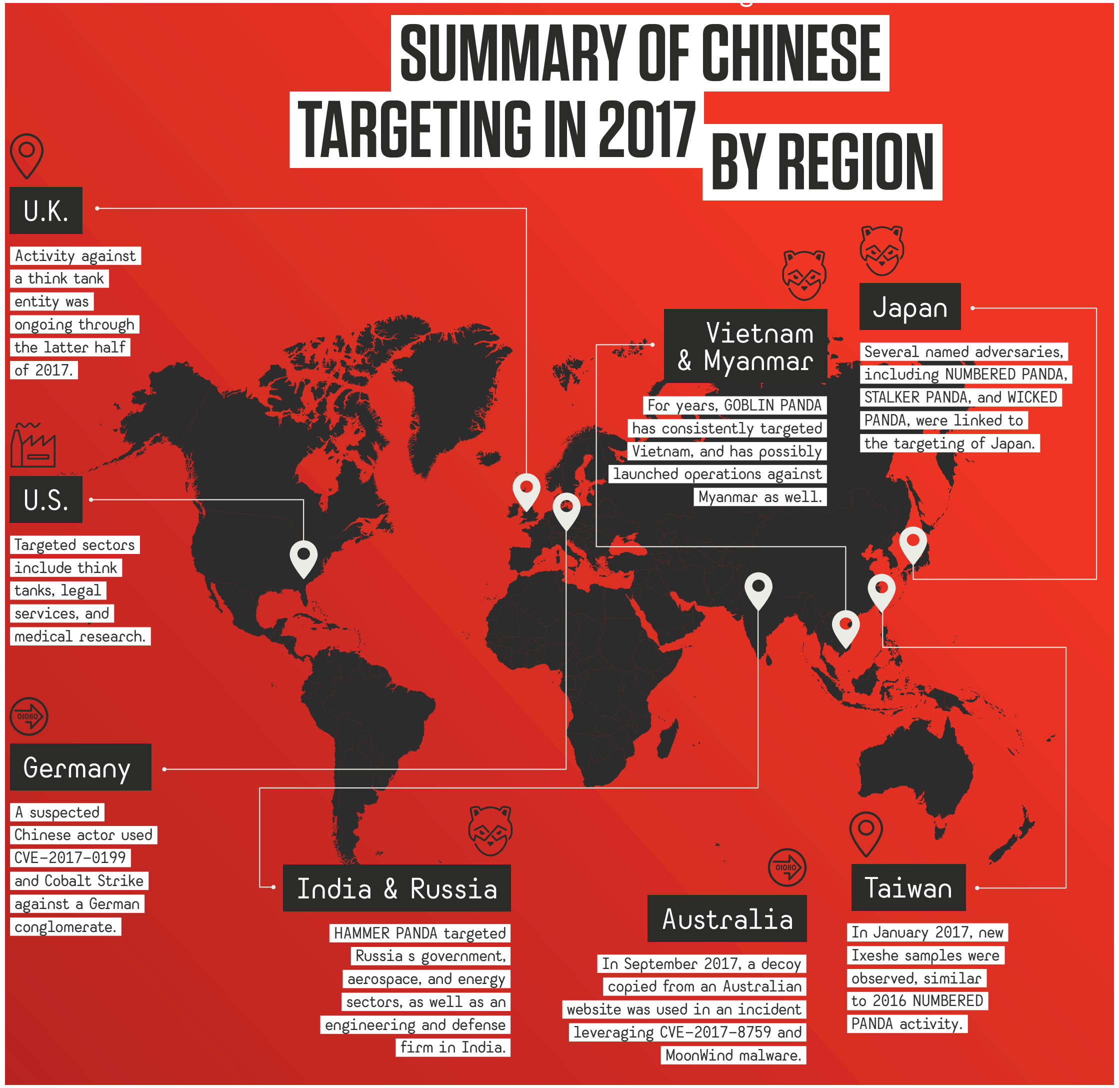
Tuesday, October 30, 2018

Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years

Chinese intelligence officers and those working under their direction, which included hackers and co-opted company insiders, conducted or otherwise enabled repeated intrusions into private companies' computer systems in the United States and abroad for over five years. The conspirators' ultimate goal was to steal, among other data, intellectual property and confidential business information, including information related to a turbofan engine used in commercial airliners.

The charged intelligence officers, Zha Rong and Chai Meng, and other co-conspirators, worked for the Jiangsu Province Ministry of State Security ("JSSD"), headquartered in Nanjing, which is a provincial foreign intelligence arm of the People's Republic of China's Ministry of State Security ("MSS"). The MSS, and by extension the JSSD, is primarily responsible for domestic counter-intelligence, non-military foreign intelligence, and aspects of political and domestic security.

China (Crowdstrike 2018)



SUMMARY OF CHINESE TARGETING IN 2017 BY REGION

U.K.

Activity against a think tank entity was ongoing through the latter half of 2017.

U.S.

Targeted sectors include think tanks, legal services, and medical research.

Germany

A suspected Chinese actor used CVE-2017-0199 and Cobalt Strike against a German conglomerate.

India & Russia

HAMMER PANDA targeted Russia s government, aerospace, and energy sectors, as well as an engineering and defense firm in India.

Vietnam & Myanmar

For years, GOBLIN PANDA has consistently targeted Vietnam, and has possibly launched operations against Myanmar as well.

Japan

Several named adversaries, including NUMBERED PANDA, STALKER PANDA, and WICKED PANDA, were linked to the targeting of Japan.

Australia

In September 2017, a decoy copied from an Australian website was used in an incident leveraging CVE-2017-8759 and MoonWind malware.

Taiwan

In January 2017, new Ixeshe samples were observed, similar to 2016 NUMBERED PANDA activity.

NEW YORK

The New York Times

PLAY THE CROSSWORD

Account

A Military Camera Said 'Made in U.S.A.' The Screen Was in Chinese.

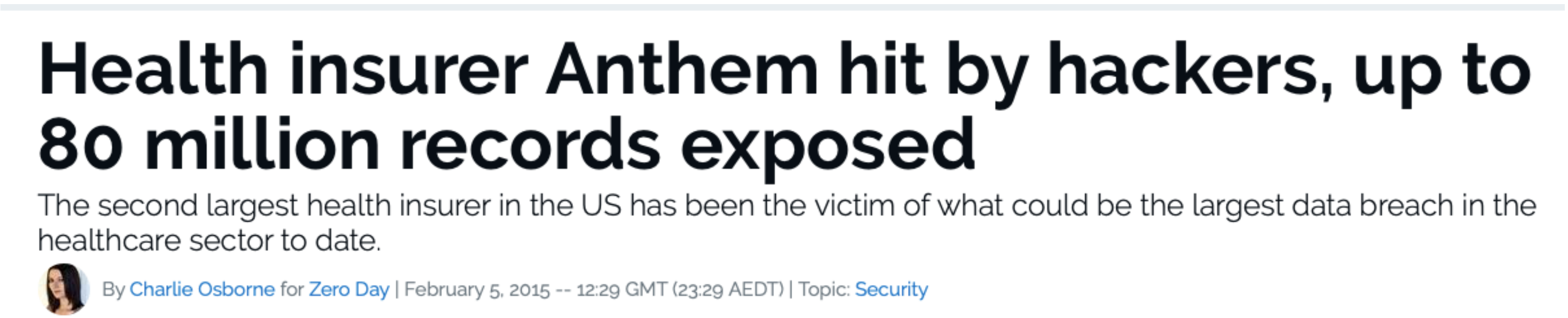
The surveillance equipment was actually manufactured in China, raising concerns that Beijing could have used it for spying, prosecutors said.

May 1, 2017 surveillance camera shipment from China to Aventura
Aventura Technologies
Aventura

Richard P. Donoghue, the United States attorney in Brooklyn, discussing the charges against the Long Island firm Aventura. Mark Lennihan/Associated Press

By Nicole Hong

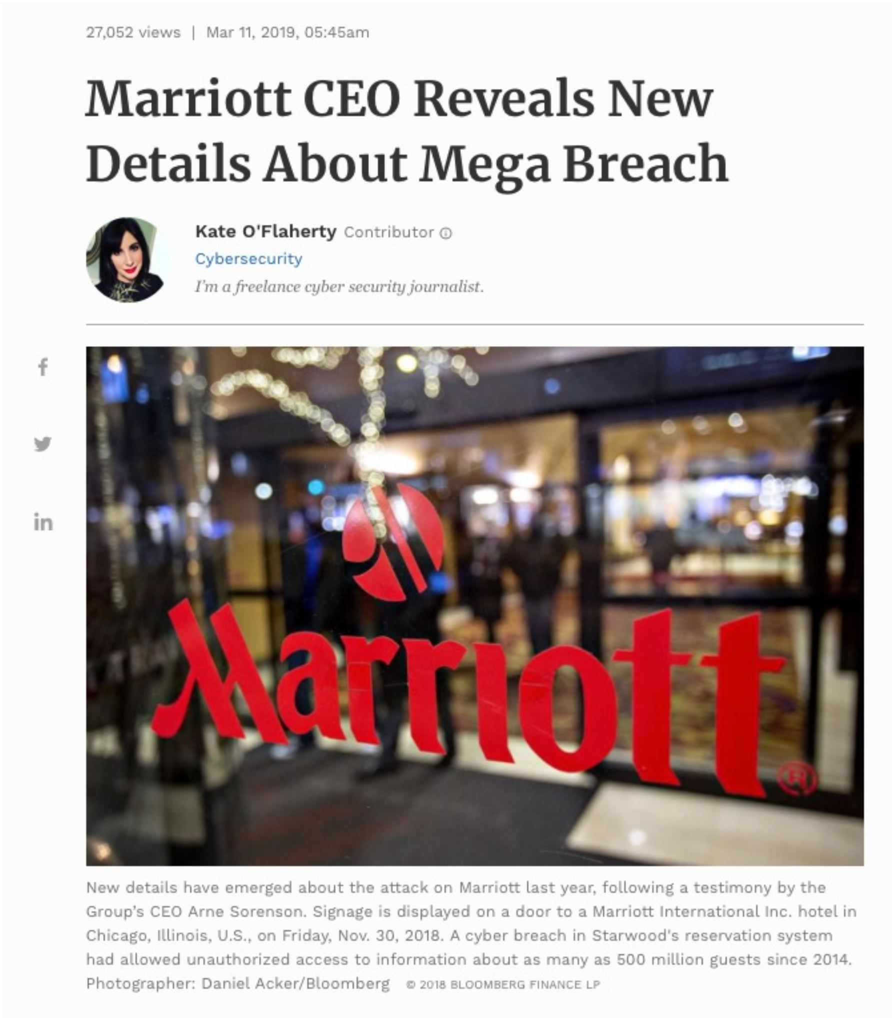
Nov. 7, 2019



Health insurer Anthem hit by hackers, up to 80 million records exposed

The second largest health insurer in the US has been the victim of what could be the largest data breach in the healthcare sector to date.

By Charlie Osborne for Zero Day | February 5, 2015 -- 12:29 GMT (23:29 AEDT) | Topic: Security



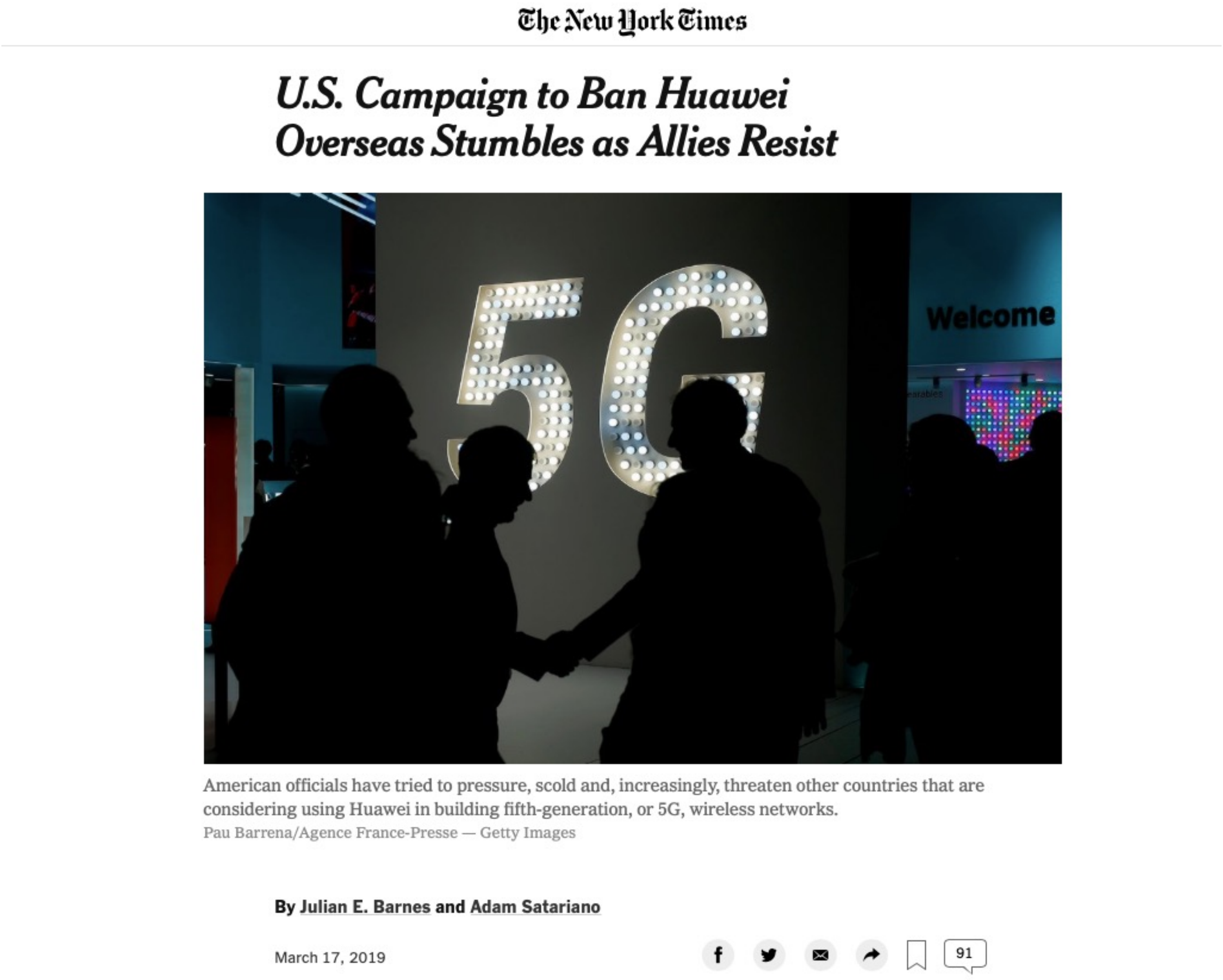
27,052 views | Mar 11, 2019, 05:45am

Marriott CEO Reveals New Details About Mega Breach

Kate O'Flaherty Contributor
Cybersecurity
I'm a freelance cyber security journalist.

New details have emerged about the attack on Marriott last year, following a testimony by the Group's CEO Arne Sorenson. Signage is displayed on a door to a Marriott International Inc. hotel in Chicago, Illinois, U.S., on Friday, Nov. 30, 2018. A cyber breach in Starwood's reservation system had allowed unauthorized access to information about as many as 500 million guests since 2014. Photographer: Daniel Acker/Bloomberg © 2018 BLOOMBERG FINANCE LP

US Efforts to Ban Huawei (NYT)



The New York Times

U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist

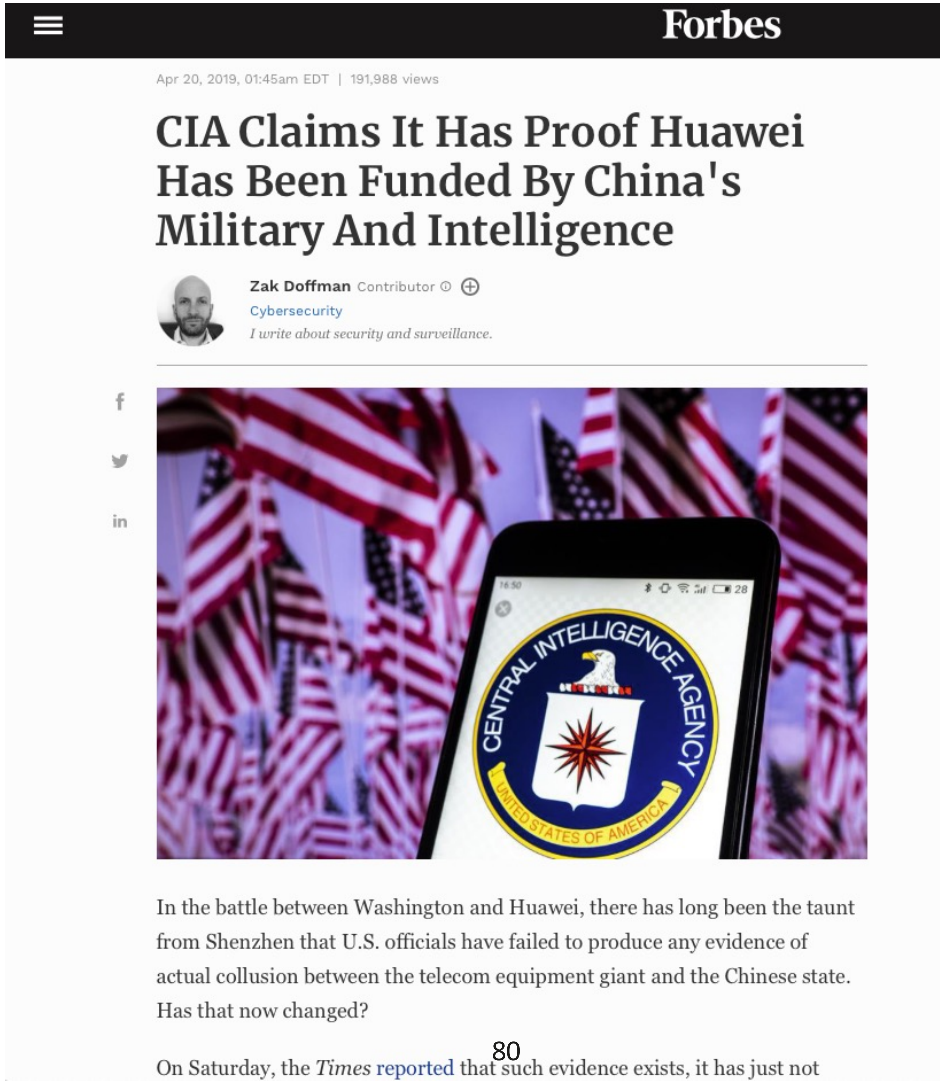
American officials have tried to pressure, scold and, increasingly, threaten other countries that are considering using Huawei in building fifth-generation, or 5G, wireless networks.

Pau Barrena/Agence France-Presse — Getty Images

By Julian E. Barnes and Adam Satariano

March 17, 2019

Huawei Funded By CCP (Forbes)



Forbes

Apr 20, 2019, 01:45am EDT | 191,988 views

CIA Claims It Has Proof Huawei Has Been Funded By China's Military And Intelligence

Zak Doffman Contributor

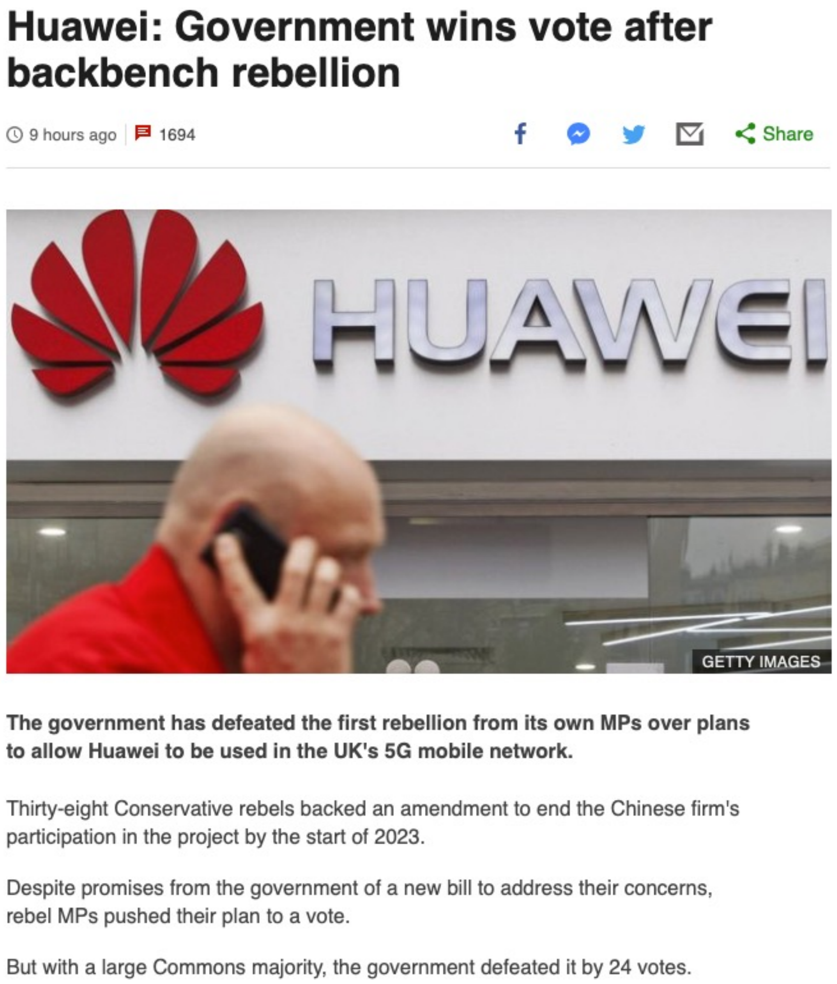
Cybersecurity

I write about security and surveillance.

In the battle between Washington and Huawei, there has long been the taunt from Shenzhen that U.S. officials have failed to produce any evidence of actual collusion between the telecom equipment giant and the Chinese state. Has that now changed?

On Saturday, the *Times* reported that such evidence exists, it has just not

News on Huawei (BBC)



Huawei: Government wins vote after backbench rebellion

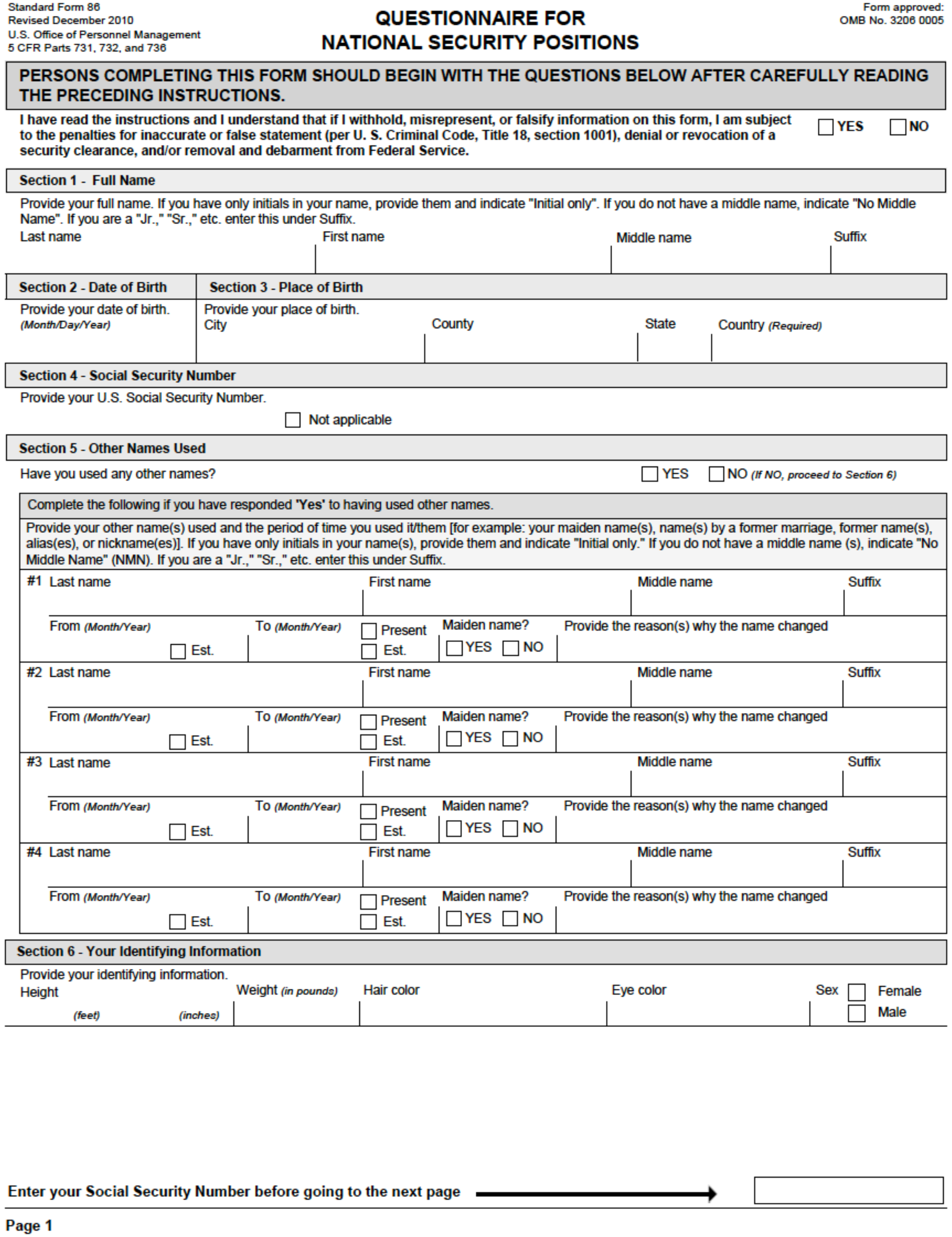
9 hours ago | 1694

The government has defeated the first rebellion from its own MPs over plans to allow Huawei to be used in the UK's 5G mobile network.

Thirty-eight Conservative rebels backed an amendment to end the Chinese firm's participation in the project by the start of 2023.

Despite promises from the government of a new bill to address their concerns, rebel MPs pushed their plan to a vote.

But with a large Commons majority, the government defeated it by 24 votes.



Standard Form 86
Revised December 2010
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

PERSONS COMPLETING THIS FORM SHOULD BEGIN WITH THE QUESTIONS BELOW AFTER CAREFULLY READING THE PRECEDING INSTRUCTIONS.

I have read the instructions and I understand that if I withhold, misrepresent, or falsify information on this form, I am subject to the penalties for inaccurate or false statement (per U. S. Criminal Code, Title 18, section 1001), denial or revocation of a security clearance, and/or removal and debarment from Federal Service. □ **YES** □ **NO**

Section 1 - Full Name

Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix.

Last name | First name | Middle name | Suffix

Section 2 - Date of Birth

Provide your date of birth. *(Month/Day/Year)*

Section 3 - Place of Birth

Provide your place of birth.
City | County | State | Country *(Required)*

Section 4 - Social Security Number

Provide your U.S. Social Security Number.

□ Not applicable

Section 5 - Other Names Used

Have you used any other names? □ YES □ NO *(If NO, proceed to Section 6)*

Complete the following if you have responded **'Yes'** to having used other names.

Provide your other name(s) used and the period of time you used it/them [for example: your maiden name(s), name(s) by a former marriage, former name(s), alias(es), or nickname(es)]. If you have only initials in your name(s), provide them and indicate "Initial only." If you do not have a middle name (s), indicate "No Middle Name" (NMN). If you are a "Jr.," "Sr.," etc. enter this under Suffix.

#1 Last name | First name | Middle name | Suffix
From *(Month/Year)* □ Est. | To *(Month/Year)* □ Present □ Est. | Maiden name? □ YES □ NO | Provide the reason(s) why the name changed

#2 Last name | First name | Middle name | Suffix
From *(Month/Year)* □ Est. | To *(Month/Year)* □ Present □ Est. | Maiden name? □ YES □ NO | Provide the reason(s) why the name changed

#3 Last name | First name | Middle name | Suffix
From *(Month/Year)* □ Est. | To *(Month/Year)* □ Present □ Est. | Maiden name? □ YES □ NO | Provide the reason(s) why the name changed

#4 Last name | First name | Middle name | Suffix
From *(Month/Year)* □ Est. | To *(Month/Year)* □ Present □ Est. | Maiden name? □ YES □ NO | Provide the reason(s) why the name changed

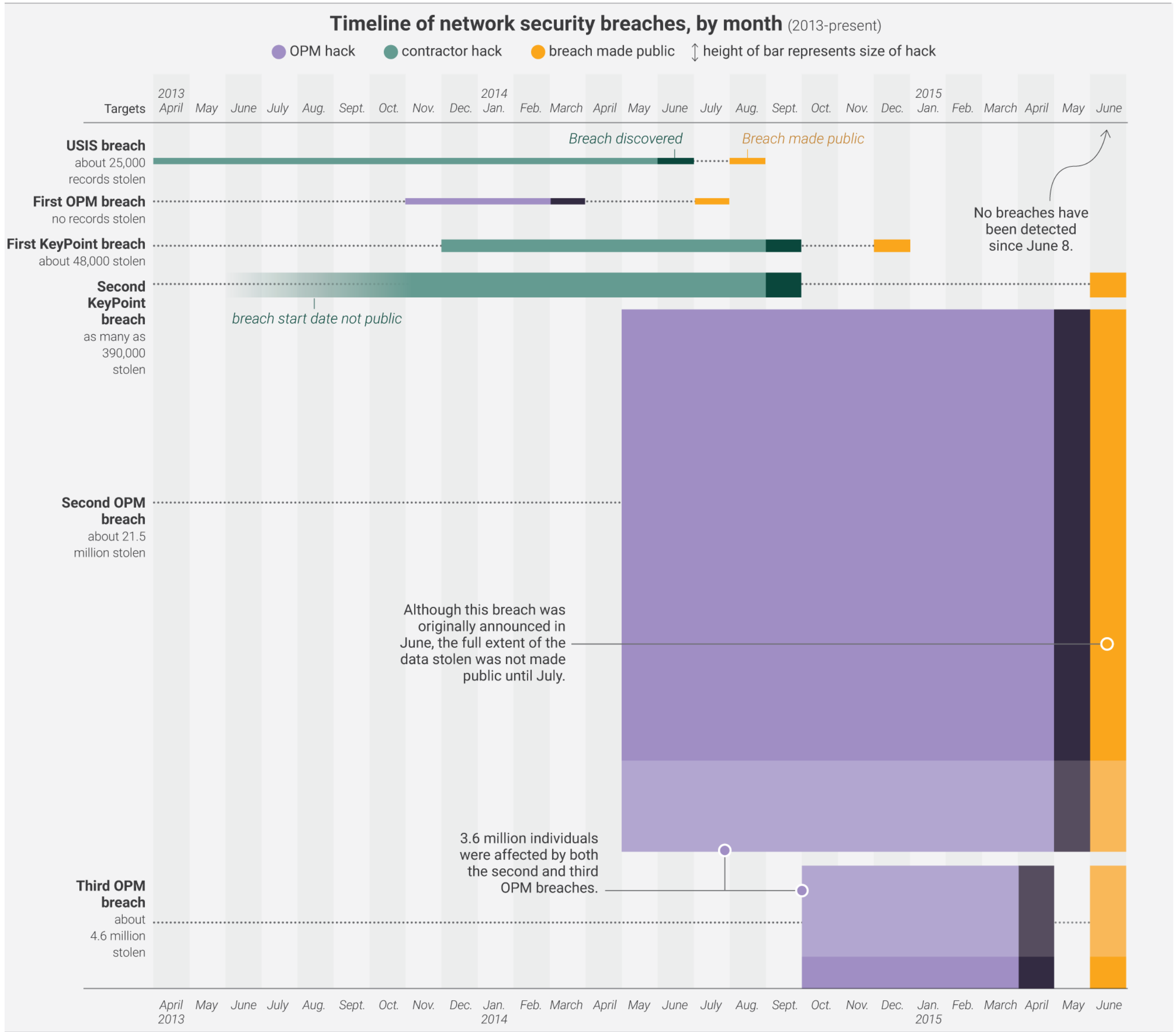
Section 6 - Your Identifying Information

Provide your identifying information.
Height *(feet)* *(inches)* | Weight *(in pounds)* | Hair color | Eye color | Sex □ Female □ Male

Enter your Social Security Number before going to the next page →

Page 1

OPM Breaches (National Journal 2016)



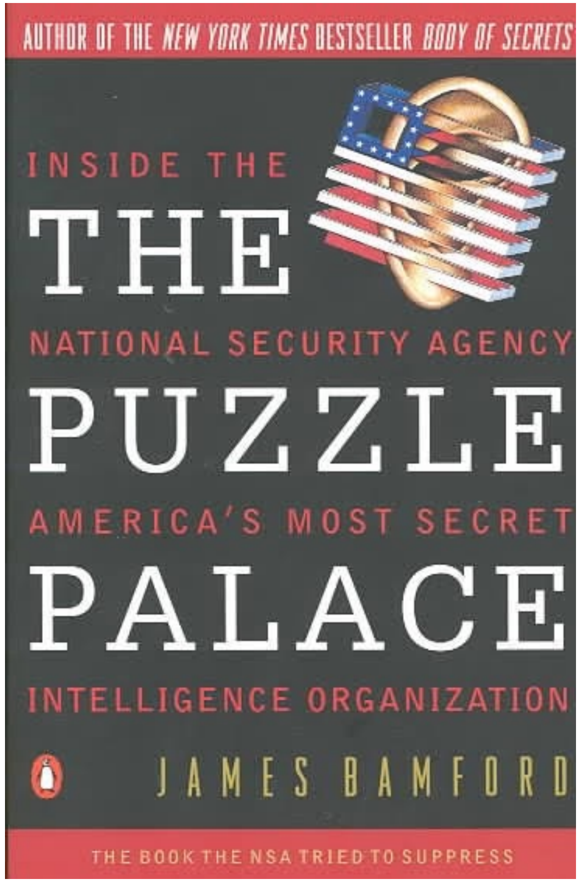
OPM Congressional Hearing (2015)

Legitimate Cyber Targets (Michael Hayden)

https://www.youtube.com/watch?v=DfyFNWOdaQA&list=PLbxnlnLusWSpIQEN5MZv0wwA7Q9xShX6Y&index=12&t=0s

USA: National Security Agency

- History dates back to WW2 code breaking and Signals Intelligence Service.
- Modern organization formed in 1952
- Puzzle Palace published in 1982 brought light to “No Such Agency”.
- Cyber world rich pickings for NSA
- Broad scope of activities revealed by Edward Snowden


AUTHOR OF THE NEW YORK TIMES BESTSELLER BODY OF SECRETS
INSIDE THE
THE
NATIONAL SECURITY AGENCY
PUZZLE
AMERICA'S MOST SECRET
PALACE
INTELLIGENCE ORGANIZATION
JAMES BAMFORD
THE BOOK THE NSA TRIED TO SUPPRESS

Who executed Stuxnet?

- NSA's Tailored Access Operations (TAO) reportedly was behind Stuxnet
- Their mission is offensive cyber operations

Need a Zero Day? (Wired 2016)

Rob Joyce head of TAO commented to a 2016 security conference,

"[With] any large network, I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero days," he says. "There's so many more vectors that are easier, less risky and quite often more productive than going down that route."

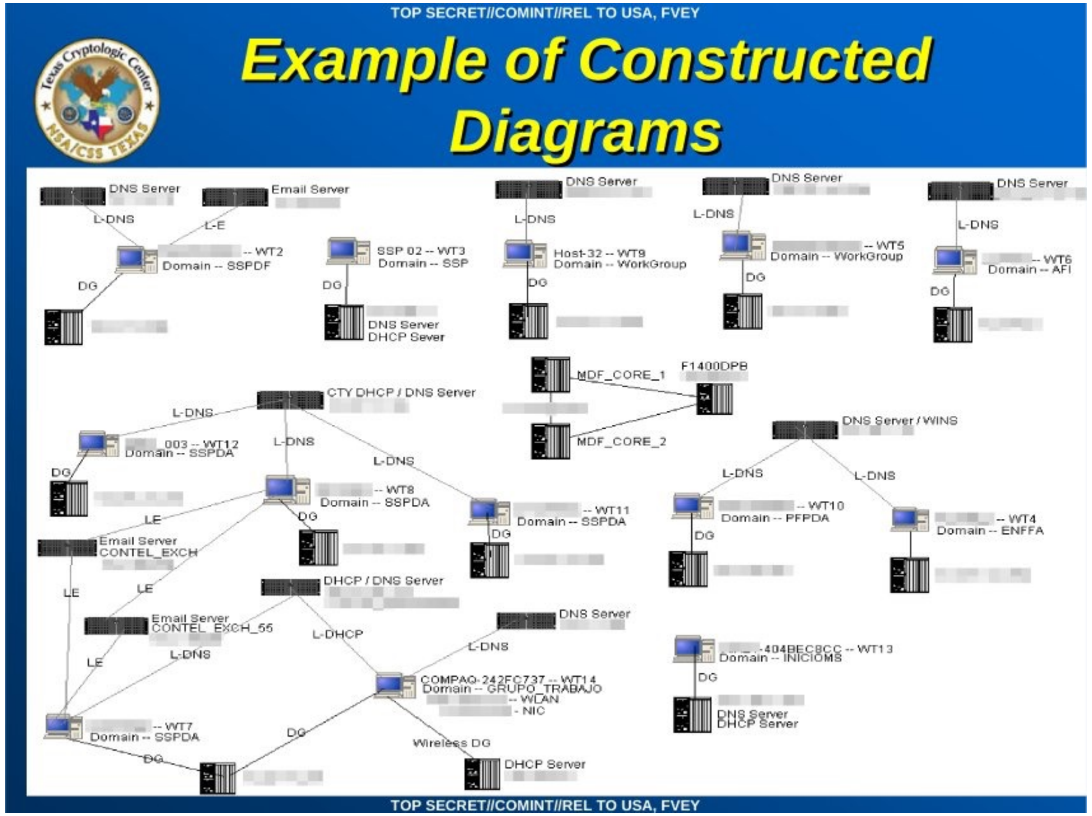
Source. wired.com

How the TAO operates (Rob Joyce NSA)

https://www.youtube.com/watch?v=bDJb8WOJYdA&list=PLbxnlnLusWSpIQEN5MZv0wwA7Q9xShX6Y&index=13&t=242s

TAO in San Antonio (der Spiegel 2013)

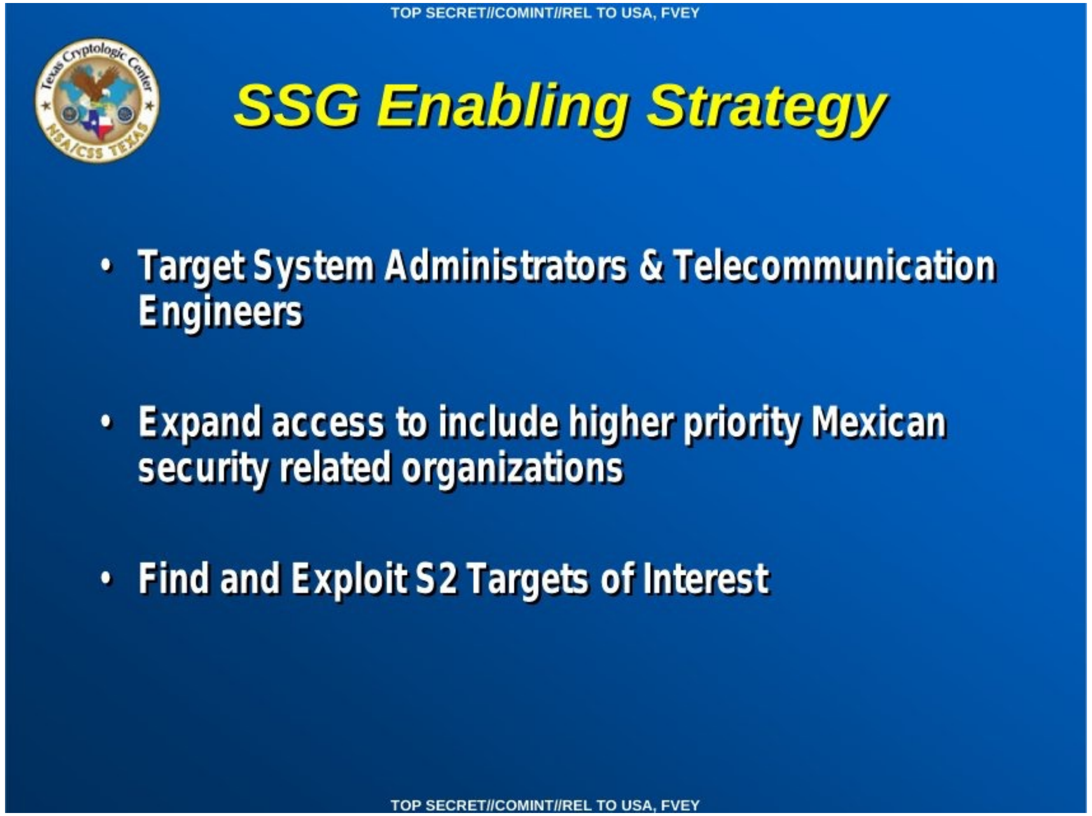
Targeting Mexican Mexico’s Secretariat of Public Security



TOP SECRET//COMINT//REL TO USA, FVEY

Example of Constructed Diagrams

TOP SECRET//COMINT//REL TO USA, FVEY



TOP SECRET//COMINT//REL TO USA, FVEY

Texas Cryptologic Center
NSA/CSS TEXAS

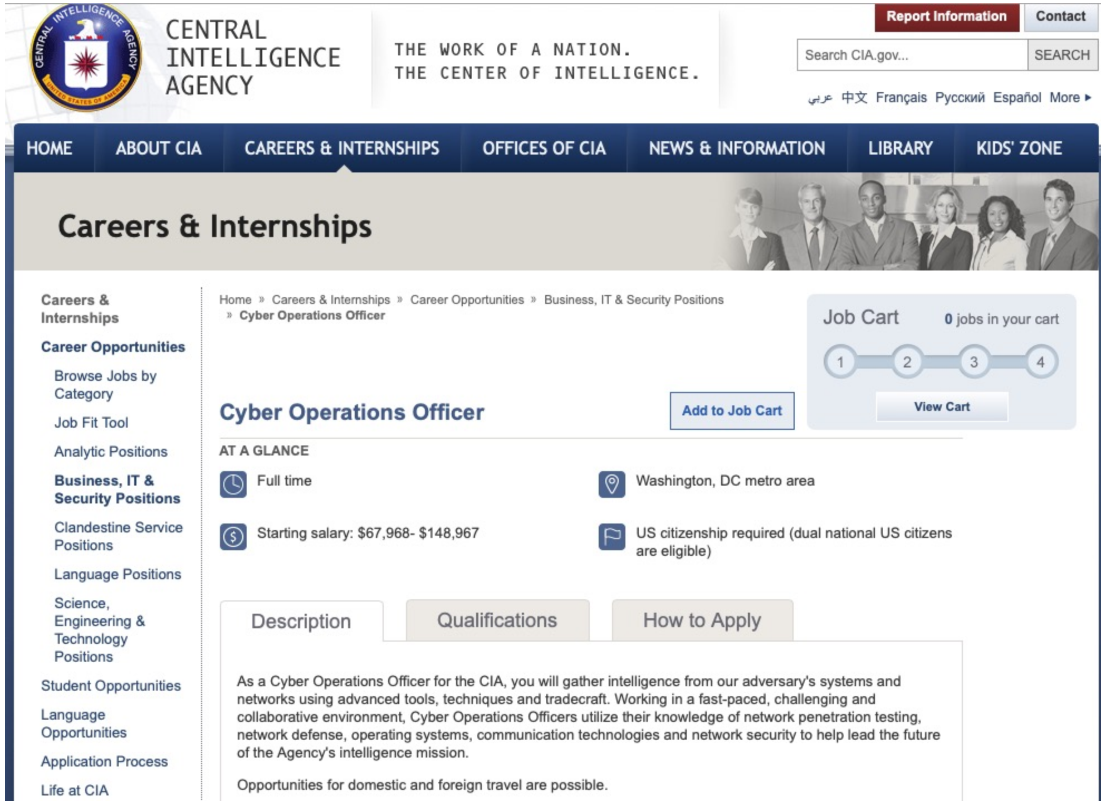
SSG Enabling Strategy

- Target System Administrators & Telecommunication Engineers
- Expand access to include higher priority Mexican security related organizations
- Find and Exploit S2 Targets of Interest

TOP SECRET//COMINT//REL TO USA, FVEY

Central Intelligence Agency

- Like other intelligence agencies CIA uses cyber extensively
- Center for Cyber Intelligence within CIA responsible for the capability
- Wikileaks Vault 7 release in 2017
- Reveals direction of global hacking program
- Information on agency’s malware arsenal
- Claims that CIA used products like iPhones and smart TVs as covert microphones



Cyber Operations Officer

AT A GLANCE

Full time

Washington, DC metro area

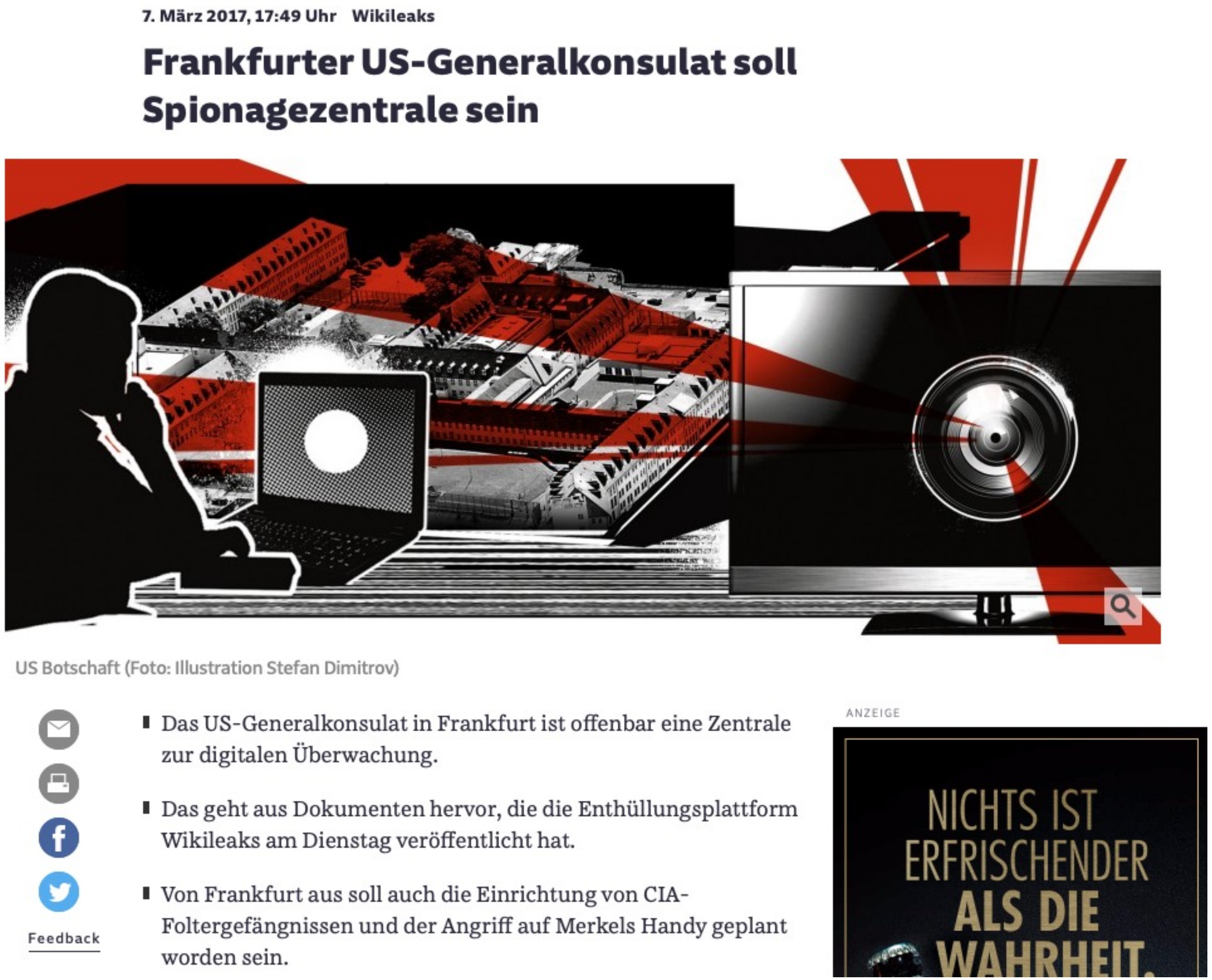
Starting salary: $67,968- $148,967

US citizenship required (dual national US citizens are eligible)

As a Cyber Operations Officer for the CIA, you will gather intelligence from our adversary's systems and networks using advanced tools, techniques and tradecraft. Working in a fast-paced, challenging and collaborative environment, Cyber Operations Officers utilize their knowledge of network penetration testing, network defense, operating systems, communication technologies and network security to help lead the future of the Agency's intelligence mission.

Opportunities for domestic and foreign travel are possible.

Frankurt Base



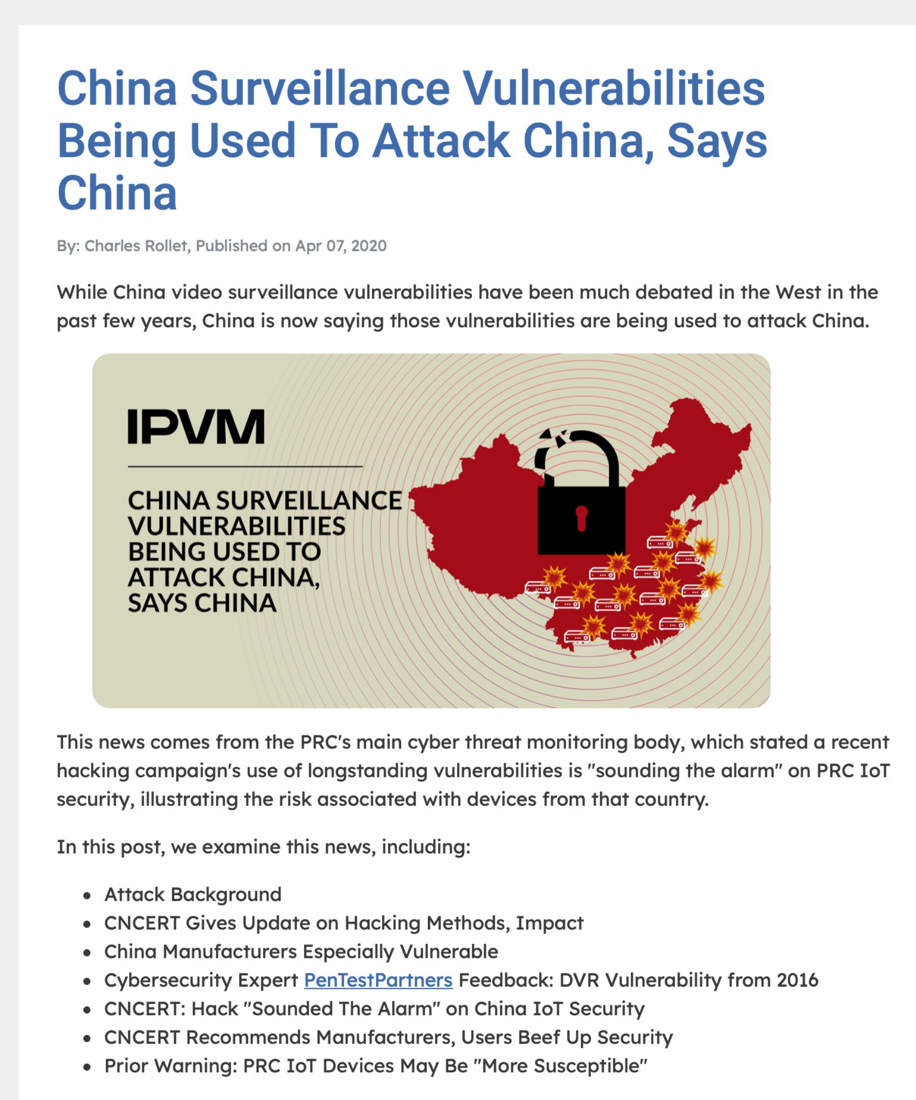
7. März 2017, 17:49 Uhr Wikileaks

Frankfurter US-Generalkonsulat soll Spionagezentrale sein

US Botschaft (Foto: Illustration Stefan Dimitrov)

- Das US-Generalkonsulat in Frankfurt ist offenbar eine Zentrale zur digitalen Überwachung.
- Das geht aus Dokumenten hervor, die die Enthüllungsplattform Wikileaks am Dienstag veröffentlicht hat.
- Von Frankfurt aus soll auch die Einrichtung von CIA-Foltergefängnissen und der Angriff auf Merkels Handy geplant worden sein.

China Under Attack (ipvm.com)



China Surveillance Vulnerabilities Being Used To Attack China, Says China

By: Charles Rollet, Published on Apr 07, 2020

While China video surveillance vulnerabilities have been much debated in the West in the past few years, China is now saying those vulnerabilities are being used to attack China.

IPVM
CHINA SURVEILLANCE VULNERABILITIES BEING USED TO ATTACK CHINA, SAYS CHINA

This news comes from the PRC's main cyber threat monitoring body, which stated a recent hacking campaign's use of longstanding vulnerabilities is "sounding the alarm" on PRC IoT security, illustrating the risk associated with devices from that country.

In this post, we examine this news, including:

- Attack Background
- CNCERT Gives Update on Hacking Methods, Impact
- China Manufacturers Especially Vulnerable
- Cybersecurity Expert PenTestPartners Feedback: DVR Vulnerability from 2016
- CNCERT: Hack "Sounded The Alarm" on China IoT Security
- CNCERT Recommends Manufacturers, Users Beef Up Security
- Prior Warning: PRC IoT Devices May Be "More Susceptible"

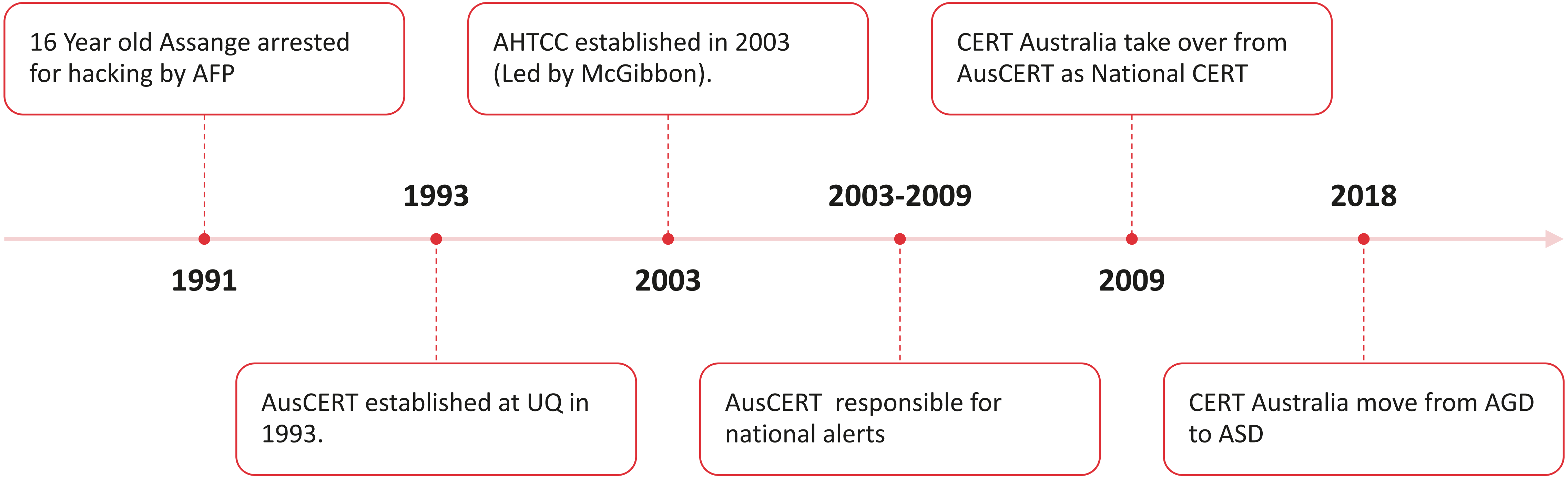
Inside US Cyber Command Video (2018)

https://www.pbs.org/video/inside-cyber-command-1522442446/

GCHQ

- Government Communications Headquarters (GCHQ)
- The UK's cyber security mission is led by the National Cyber Security Centre (NCSC), which is a part of GCHQ.
- “Effects - we have a range of online capabilities that can lead to a real world outcome (GCHQ 2019). ”
- Operation Socialist 2010 -2013

Australian Timeline



1991

16 Year old Assange arrested for hacking by AFP

1993

AusCERT established at UQ in 1993.

2003

AHTCC established in 2003 (Led by McGibbon).

2003-2009

AusCERT responsible for national alerts

2009

CERT Australia take over from AusCERT as National CERT

2018

CERT Australia move from AGD to ASD

Australian Signals Directorate (ASD)

- ASD formerly DSD
- Similar role to GCHQ
- Increasingly involved in Cyber since 2000s
- Snowden revealed they spied on PNG military despite the close ties
- Defence and ASD replaced AFP as prime for cyber response
- ASD took over CERT Australia from AGs and ACSC now has offensive cyber in role

ASD
AUSTRALIAN SIGNALS DIRECTORATE

ACSC
Australian
Cyber Security
Centre

ISIS Cyber Attacks

LOWY INSTITUTE
Mike Burgess, Director-General of the Australian Signals Directorate (ASD...
Watch later
Share
MORE VIDEOS
7:30 / 59:12
CC
YouTube

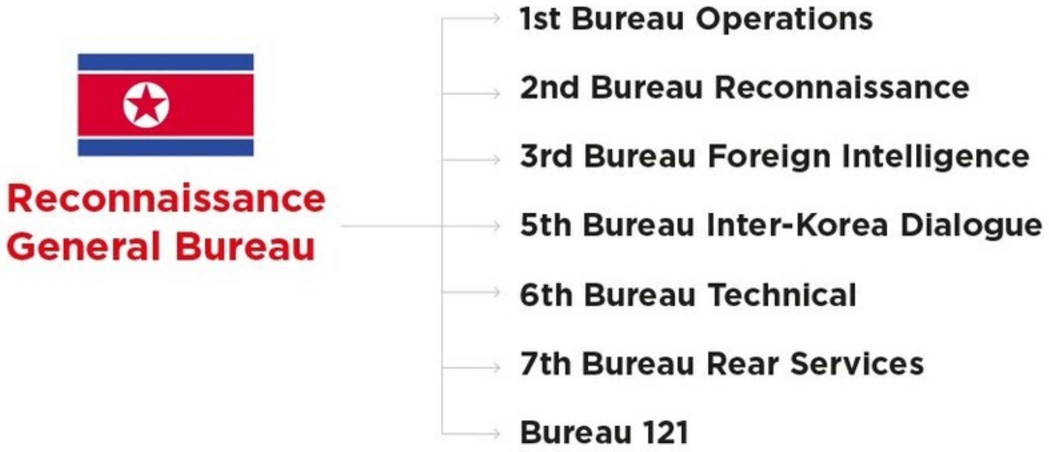
https://www.lowyinstitute.org/news-and-media/multimedia/video/mike-burgess-director-general-australian-signals-directorate-asd

North Korea

- Cyber threats from the North Korean government are significant and increasing, but are less sophisticated than threats posed by countries such as China or Russia.
- The government has demonstrated a willingness to engage in seemingly reckless and sometimes destructive operations without regard for international norms and consequences.

North Korea

- North Korean operations primarily target organisations in South Korea.
- However, organisations in countries that North Korea considers strategically important, particularly the United States and Japan are also targeted
- The North Korean government's cyber capabilities are drawn exclusively from its intelligence agencies and subordinate offices; there is no civilian hacking community in North Korea.



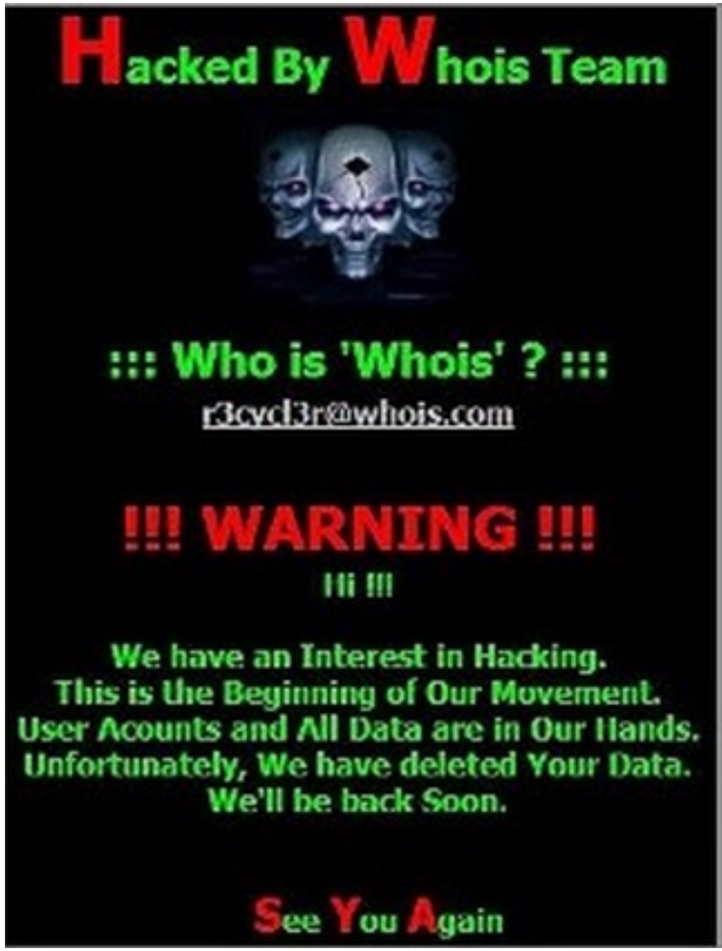
Reconnaissance General Bureau

- 1st Bureau Operations
- 2nd Bureau Reconnaissance
- 3rd Bureau Foreign Intelligence
- 5th Bureau Inter-Korea Dialogue
- 6th Bureau Technical
- 7th Bureau Rear Services
- Bureau 121

North Korea

- Analysis suggests that North Korea leverages these agencies' cyber capabilities to achieve the following objectives:
  - sabotage and disruption
  - political, military, and economic intelligence gathering
  - government-sponsored criminal moneymaking
- One former British intelligence chief estimates the take from its cyber-heists may bring the North as much as $1 billion a year, or a third of the value of the nation’s exports (Source: NYT 2018)

Darkseoul 2013 (KrebsonSecurity)



Hacked By Whois Team

::: Who is 'Whois' ? :::

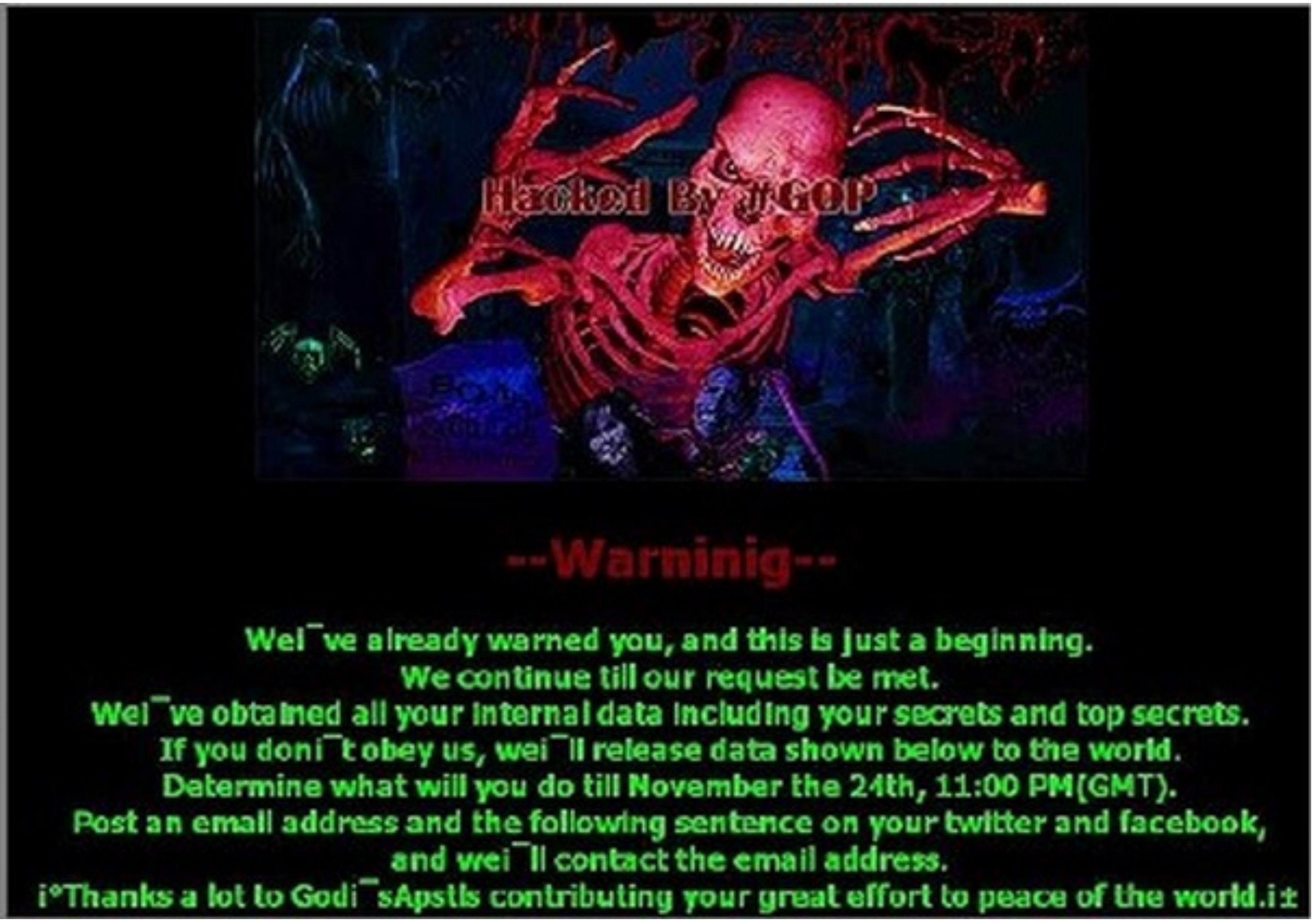
r3cycl3r@whois.com

!!! WARNING !!!

Hi !!!

We have an Interest in Hacking.
This is the Beginning of Our Movement.
User Acounts and All Data are in Our Hands.
Unfortunately, We have deleted Your Data.
We'll be back Soon.

See You Again



--Warninig--

Wei¯ve already warned you, and this is just a beginning.
We continue till our request be met.
Wei¯ve obtained all your internal data including your secrets and top secrets.
If you doni¯t obey us, wei¯ll release data shown below to the world.
Determine what will you do till November the 24th, 11:00 PM(GMT).
Post an email address and the following sentence on your twitter and facebook,
and wei¯ll contact the email address.
i°Thanks a lot to Godi¯sApstls contributing your great effort to peace of the world.i±

The Interview 2014 (amazon.com)

전쟁은 시작될것이다
전쟁은 시작될것이다
THE INTERVIEW

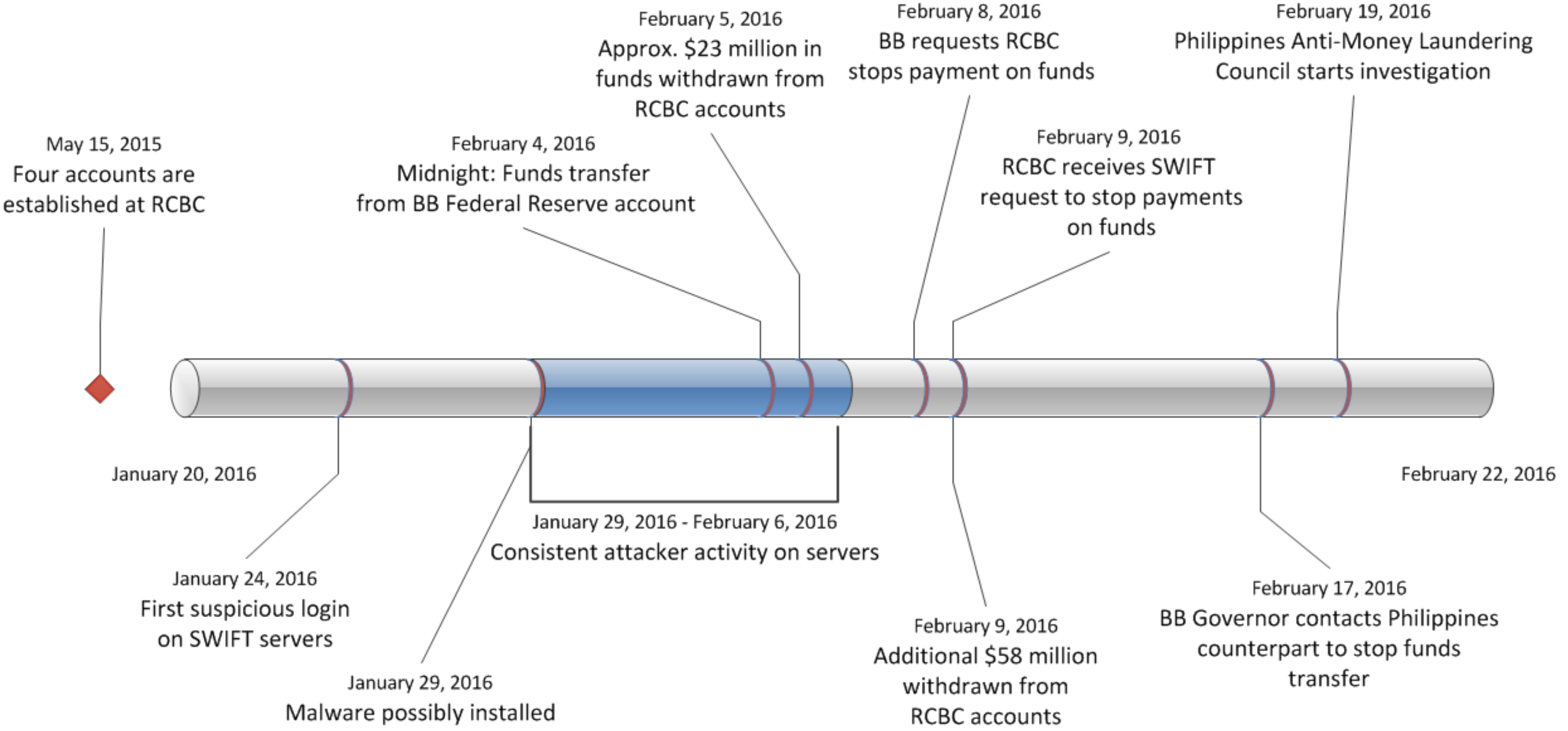
Perfect Weapon – Sony Hack

- https://youtu.be/t4H6sjMis_s?list=PLbxnlnLusWSpIQEN5MZv0wwA7Q9xShX6Y

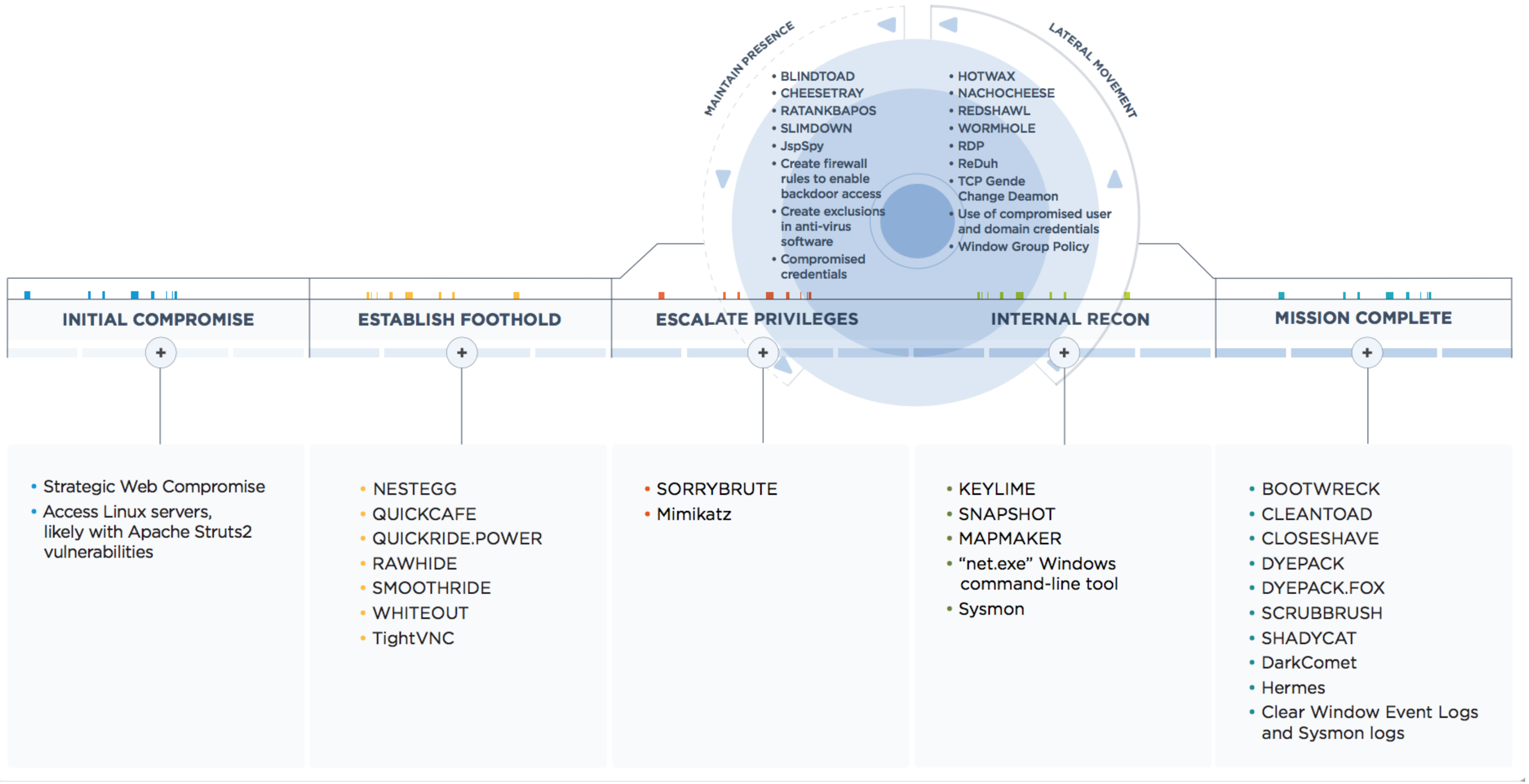
Cybercrime of the SWIFT interbank network 2016 (Langdale)

- In February 2016 computer hackers stole over US $100 million from the Bangladesh Bank by sending requests to the U.S. Federal Reserve in New York for around US $1 billion
- Fortunately most of the requests were denied and of the $100 million that was stolen around $20 million was detected and returned
- Subsequently, another $18 billion was recovered, but the rest has disappeared

North Korean Attack on Swift (Secureworks)


May 15, 2015
Four accounts are established at RCBC
February 4, 2016
Midnight: Funds transfer from BB Federal Reserve account
February 5, 2016
Approx. $23 million in funds withdrawn from RCBC accounts
February 8, 2016
BB requests RCBC stops payment on funds
February 9, 2016
RCBC receives SWIFT request to stop payments on funds
February 19, 2016
Philippines Anti-Money Laundering Council starts investigation
January 20, 2016
February 22, 2016
January 24, 2016
First suspicious login on SWIFT servers
January 29, 2016
Malware possibly installed
January 29, 2016 - February 6, 2016
Consistent attacker activity on servers
February 9, 2016
Additional $58 million withdrawn from RCBC accounts
February 17, 2016
BB Governor contacts Philippines counterpart to stop funds transfer

APT38 Attack Lifecycle (Mandiant 2018)



- BLINDTOAD
- CHEESETRAY
- RATANKBAPOS
- SLIMDOWN
- JspSpy
- Create firewall rules to enable backdoor access
- Create exclusions in anti-virus software
- Compromised credentials

- HOTWAX
- NACHOCHEESE
- REDSHAWL
- WORMHOLE
- RDP
- ReDuh
- TCP Gende Change Deamon
- Use of compromised user and domain credentials
- Window Group Policy

INITIAL COMPROMISE

- Strategic Web Compromise
- Access Linux servers, likely with Apache Struts2 vulnerabilities

ESTABLISH FOOTHOLD

- NESTEGG
- QUICKCAFE
- QUICKRIDE.POWER
- RAWHIDE
- SMOOTHRIDE
- WHITEOUT
- TightVNC

ESCALATE PRIVILEGES

- SORRYBRUTE
- Mimikatz

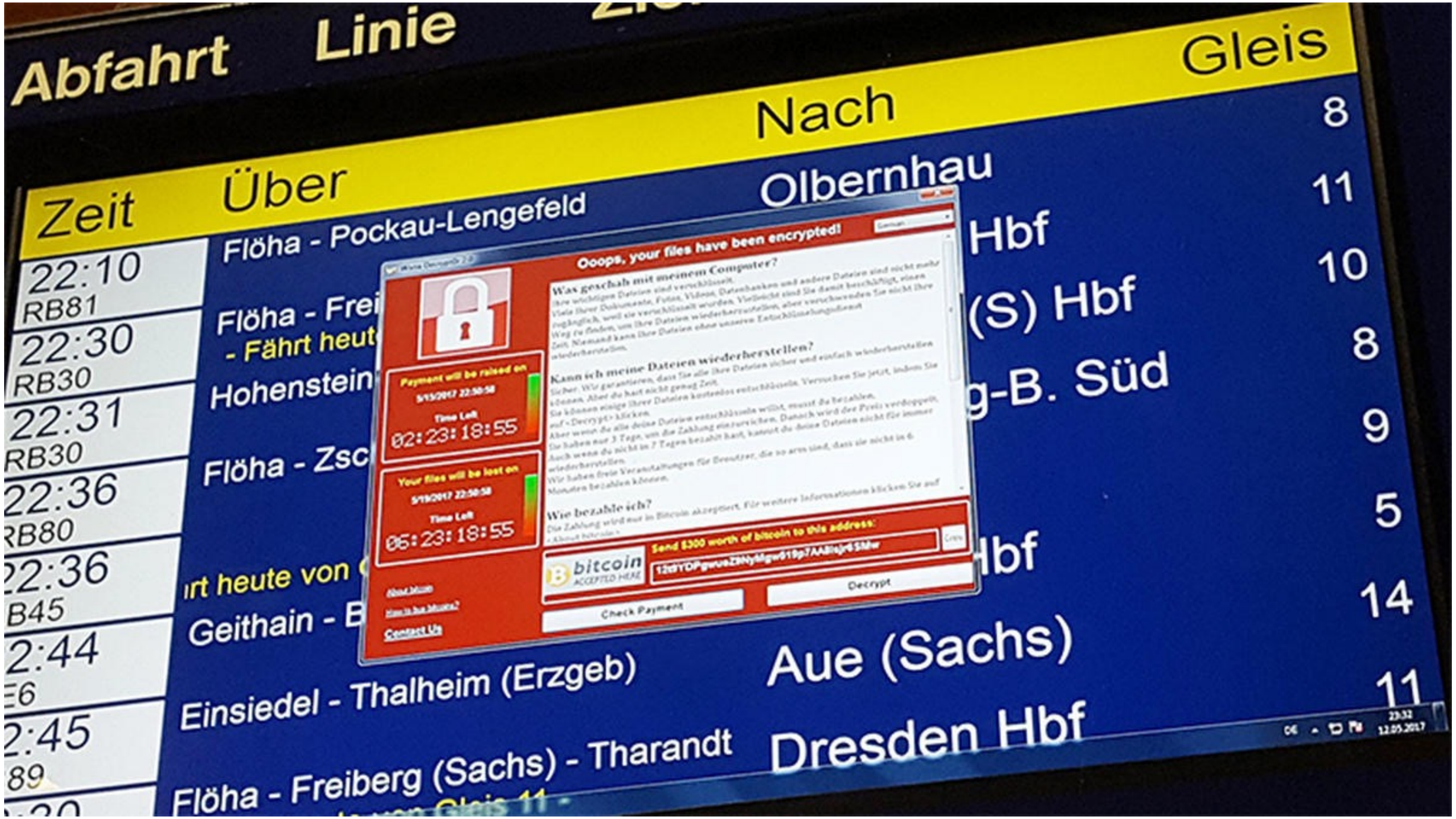
INTERNAL RECON

- KEYLIME
- SNAPSHOT
- MAPMAKER
- “net.exe” Windows command-line tool
- Sysmon

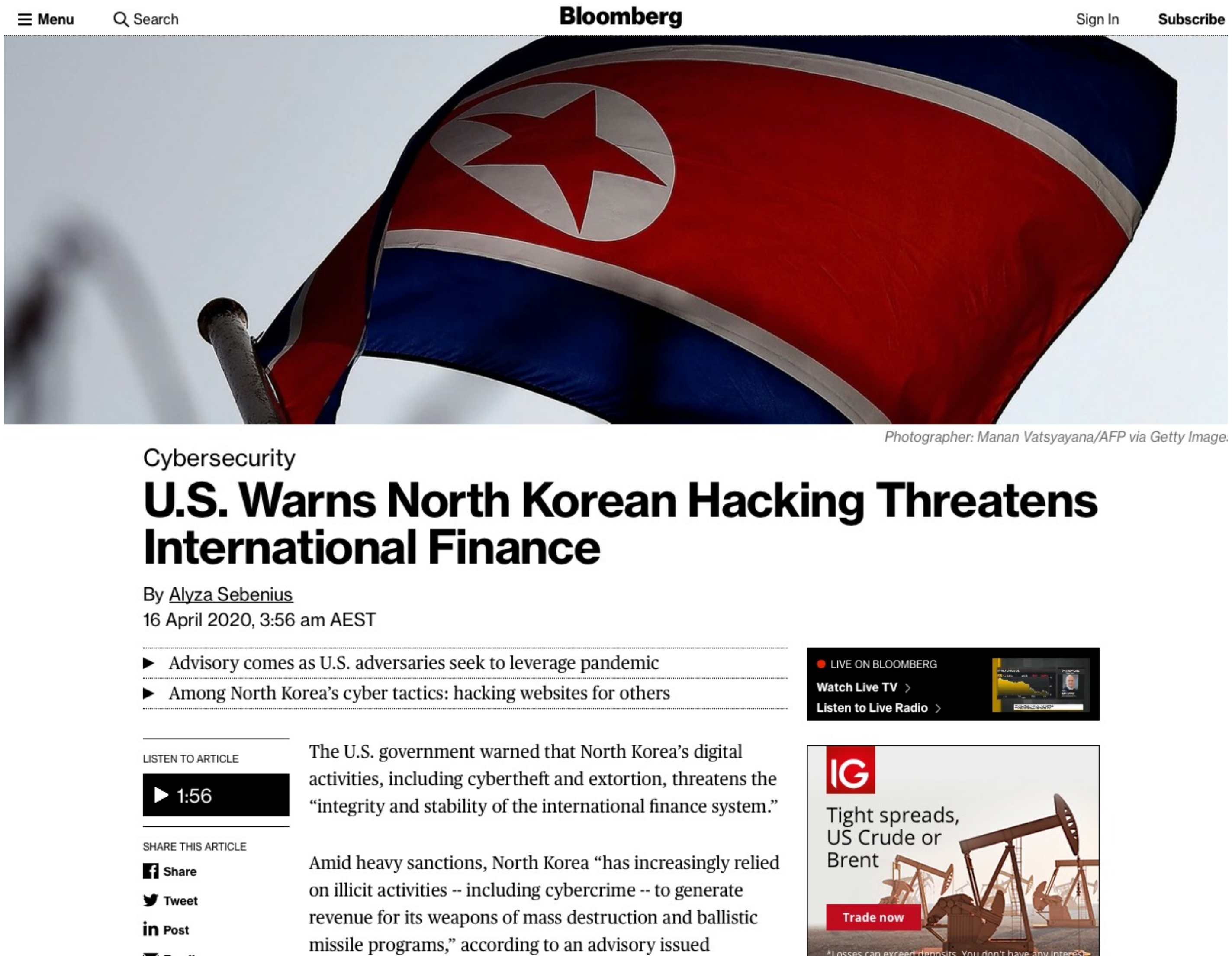
MISSION COMPLETE

- BOOTWRECK
- CLEANTOAD
- CLOSESHAVE
- DYEPACK
- DYEPACK.FOX
- SCRUBBRUSH
- SHADYCAT
- DarkComet
- Hermes
- Clear Window Event Logs and Sysmon logs

Wannacry (ZDnet 2017)



Threats to Banking (Bloomberg)



Photographer: Manan Vatsyayana/AFP via Getty Image

Cybersecurity

U.S. Warns North Korean Hacking Threatens International Finance

By Alyza Sebenius
16 April 2020, 3:56 am AEST

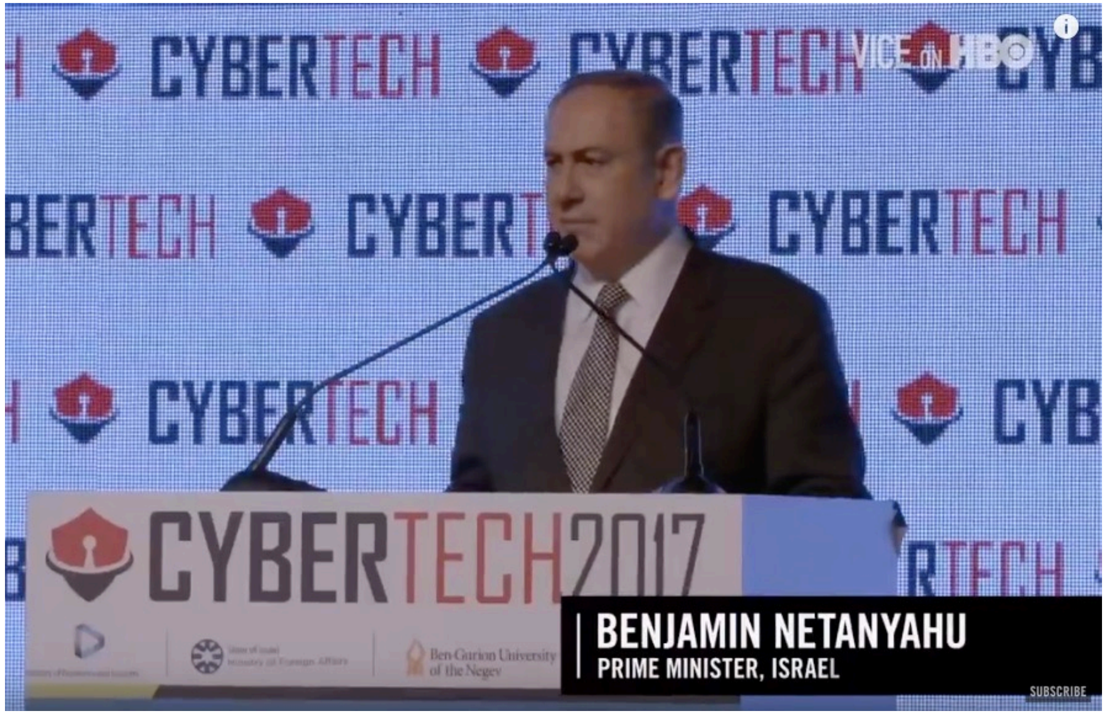
- Advisory comes as U.S. adversaries seek to leverage pandemic
- Among North Korea's cyber tactics: hacking websites for others

The U.S. government warned that North Korea's digital activities, including cybertheft and extortion, threatens the "integrity and stability of the international finance system."

Amid heavy sanctions, North Korea "has increasingly relied on illicit activities -- including cybercrime -- to generate revenue for its weapons of mass destruction and ballistic missile programs," according to an advisory issued

Israel

- Israel has a highly advanced cyber capability both for defence and offence
- Its most famous Unit 8200 is part of the Israeli military and was a signals intelligence organisation much like the NSA and GCHQ
- Unit 8200 worked with NSA to develop and deliver Stuxnet
- Many former Unit 8200 personnel work in the burgeoning Israeli cyber security industry



vice.com

Unit 8200 Recruiting & Operations in Palestinian Territories

יחידה 8200

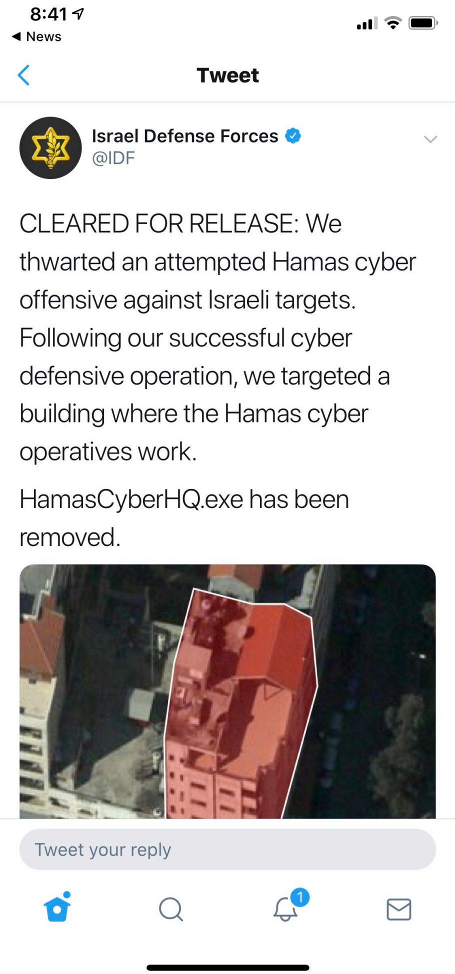
https://video.vice.com/en_us/video/how-israel-rules-the-world-of-cyber-security/5a565b99177dd47339271be1 5.53

Yoel Guzanksy Israeli NSC

- *“..(Cyber operations) involve pinpointing and surgically targeting the specific nuclear threat while minimizing the collateral damage. The idea is that each operation, in and of itself, isn’t blatant or overwhelming enough to force Iran to react. But these attacks also deliver a message to Iran that whoever is behind them has direct access to nuclear and military assets within the country. The demonstrated ability to penetrate Iranian territory and facilities underscores Iranian vulnerability to the suspected attacker’s long reach. As such, beyond any delays to Iran’s program, this demonstrated “invisible hand” has a psychological effect, which enhances Iran’s sense of paranoia that any equipment malfunction might very well be due to external intervention.”*

(Source: http://the-diplomat.com/2011/12/09/the-trick-to-sabotaging-iran/)

IDF respond to Cyber with Kinetic Strike (IDF 2019)

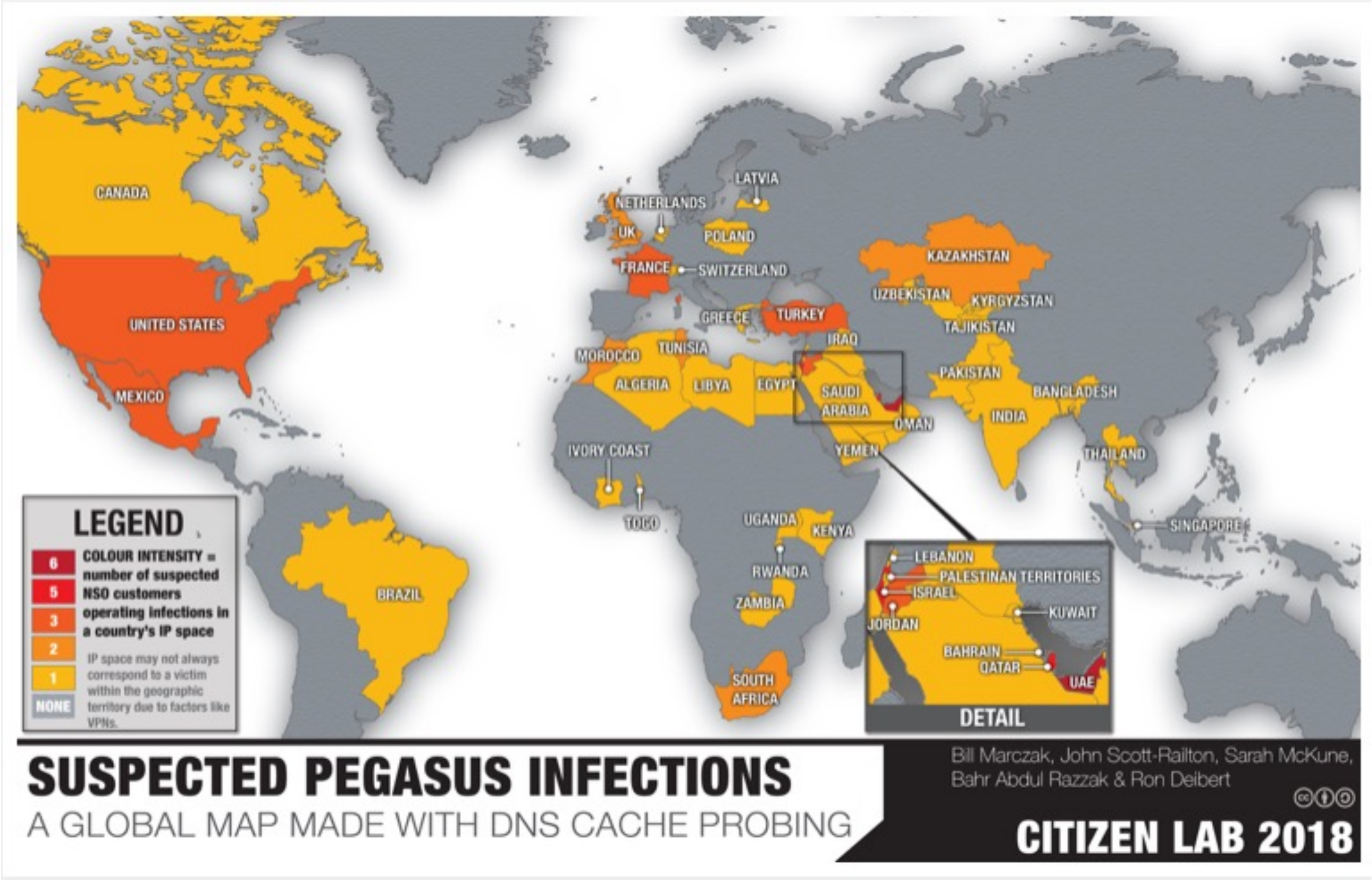


CLEARED FOR RELEASE: We thwarted an attempted Hamas cyber offensive against Israeli targets. Following our successful cyber defensive operation, we targeted a building where the Hamas cyber operatives work.

HamasCyberHQ.exe has been removed.

https://youtu.be/k2YmLYZVQGo?list=PLbxnlnLusWSpIQEN5MZv0wwA7Q9xShX6Y

NSO Group (Citizen Lab 2018)



SUSPECTED PEGASUS INFECTIONS

A GLOBAL MAP MADE WITH DNS CACHE PROBING

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak & Ron Deibert

CITIZEN LAB 2018

Iran

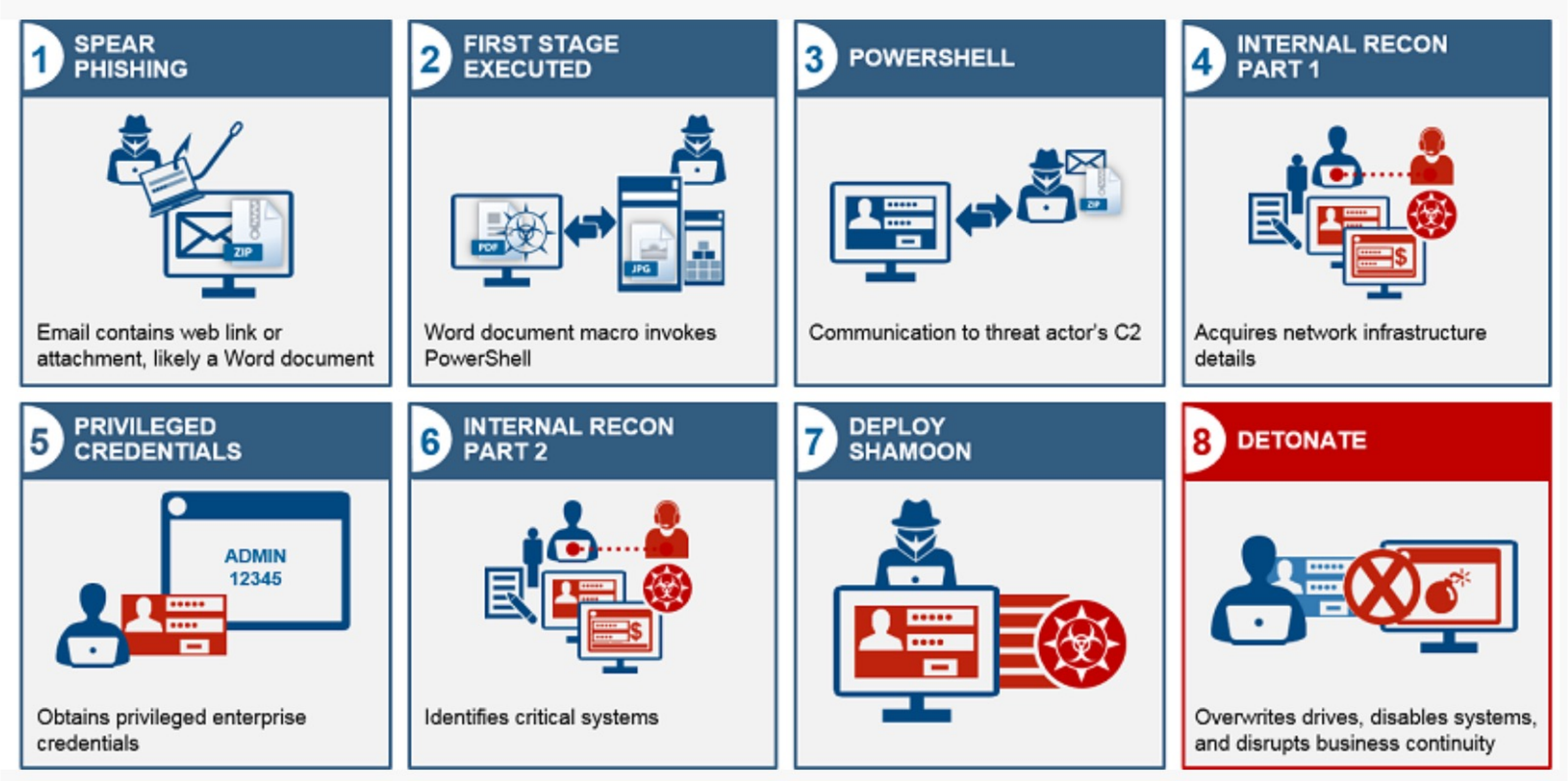
- Iran has developed its cyber capability rapidly
- While some patriotic hackers existing in the early 2000s Iran was late to the game
- The cyber units within the Iranian Revolutionary Guard are an outgrowth of Iran’s response to Stuxnet, Flame and Gauss

Cbsnews.com

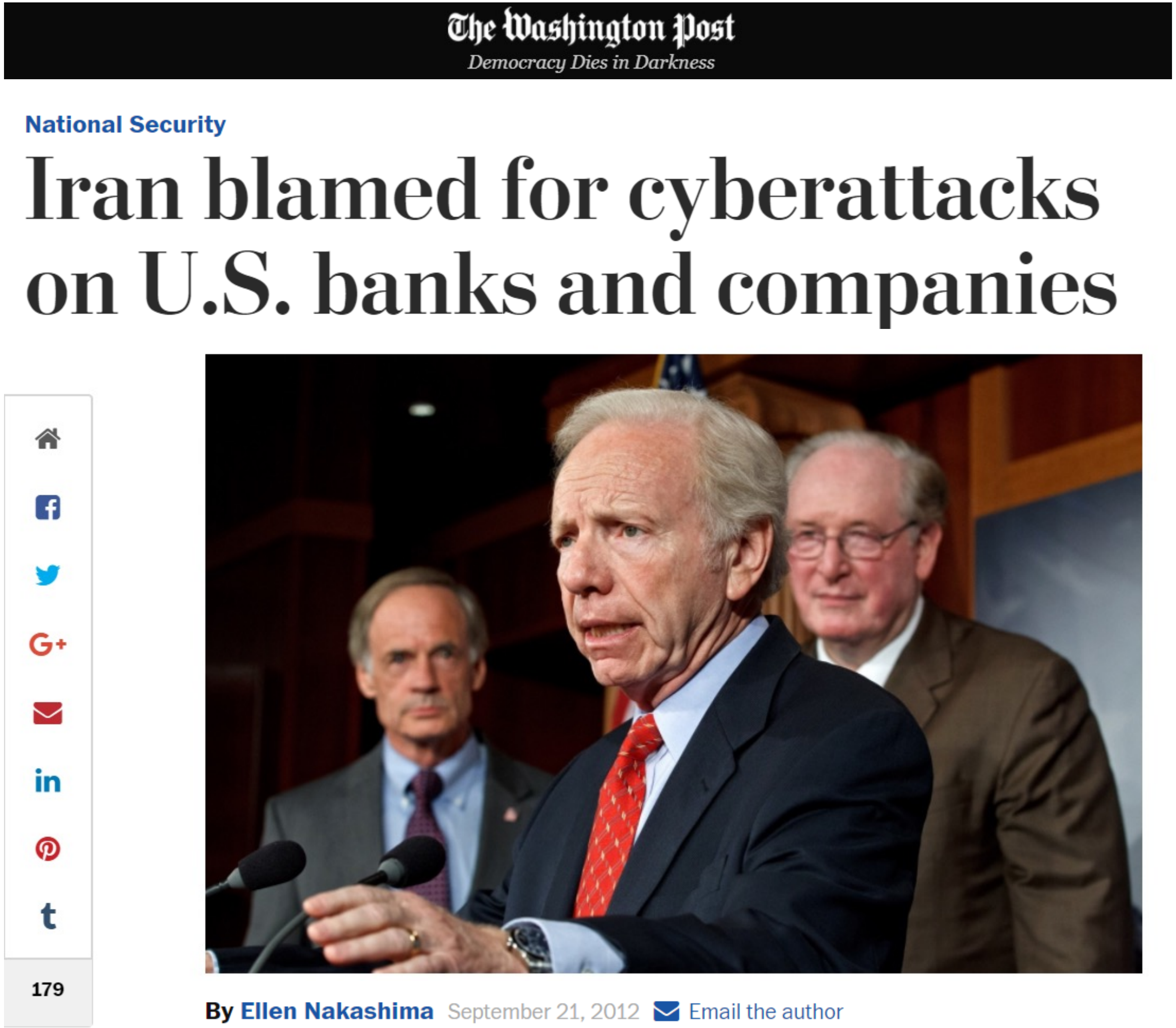
Shamoon 2012

- Saudi Aramco & Qatar Gas IT networks were targeted by destructive malware Shamoon as a response by Iran after Stuxnet.
- The malware wiped 30,000 hard disks in the process.
- While Aramco’s OT network was unaffected all their business systems were down.
- They had to give away oil over a month.

Shamoon (IBM)



1 SPEAR PHISHING
ZIP
Email contains web link or attachment, likely a Word document
2 FIRST STAGE EXECUTED
PDF
JPG
Word document macro invokes PowerShell
3 POWERSHELL
ZIP
Communication to threat actor's C2
4 INTERNAL RECON PART 1
Acquires network infrastructure details
5 PRIVILEGED CREDENTIALS
ADMIN
12345
Obtains privileged enterprise credentials
6 INTERNAL RECON PART 2
Identifies critical systems
7 DEPLOY SHAMOON
8 DETONATE
Overwrites drives, disables systems, and disrupts business continuity



The Washington Post

Democracy Dies in Darkness

National Security

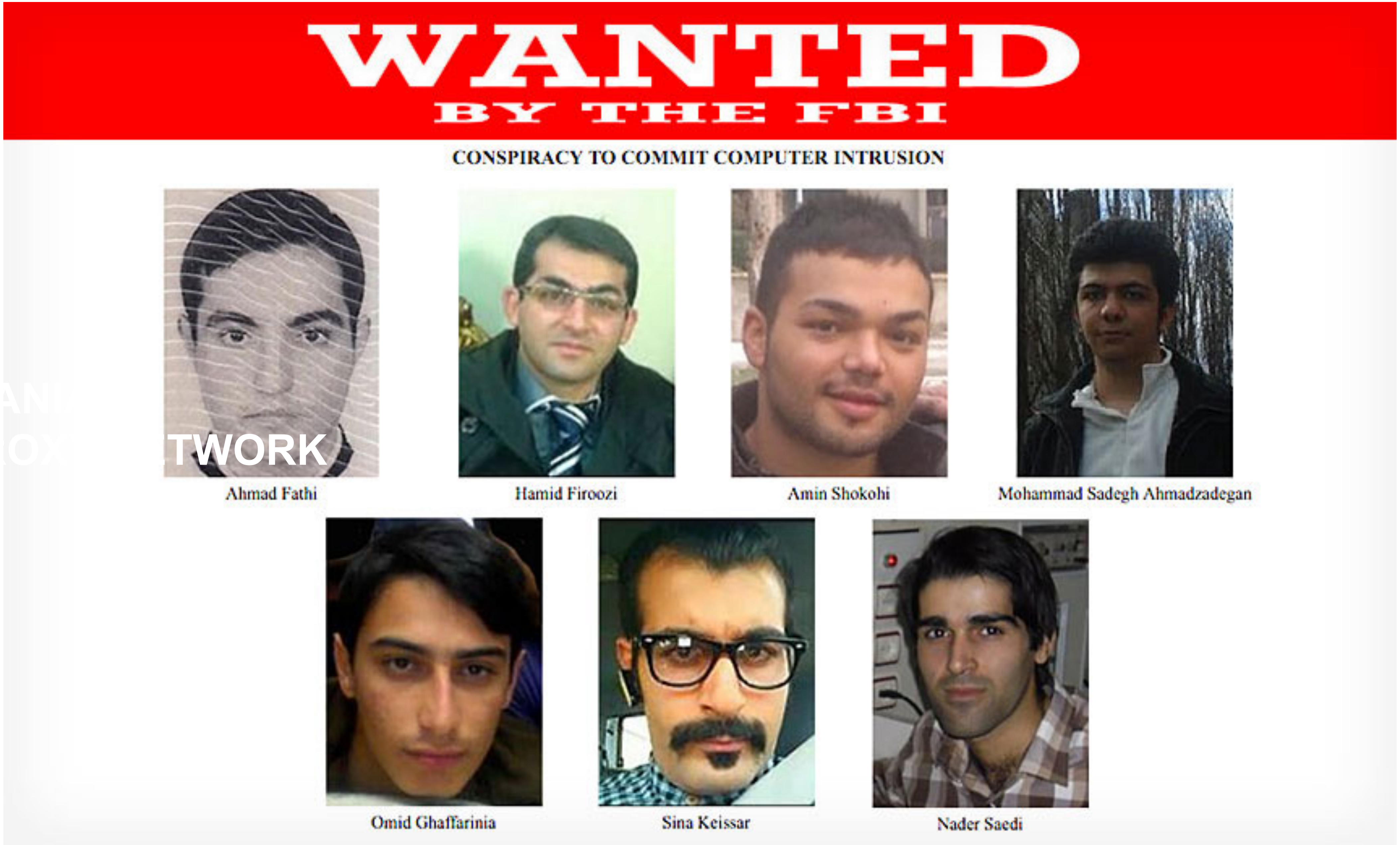
Iran blamed for cyberattacks on U.S. banks and companies

179

By Ellen Nakashima September 21, 2012 Email the author

ANI

ROX TWORK



WANTED

BY THE FBI

CONSPIRACY TO COMMIT COMPUTER INTRUSION

Ahmad Fathi

Hamid Firoozi

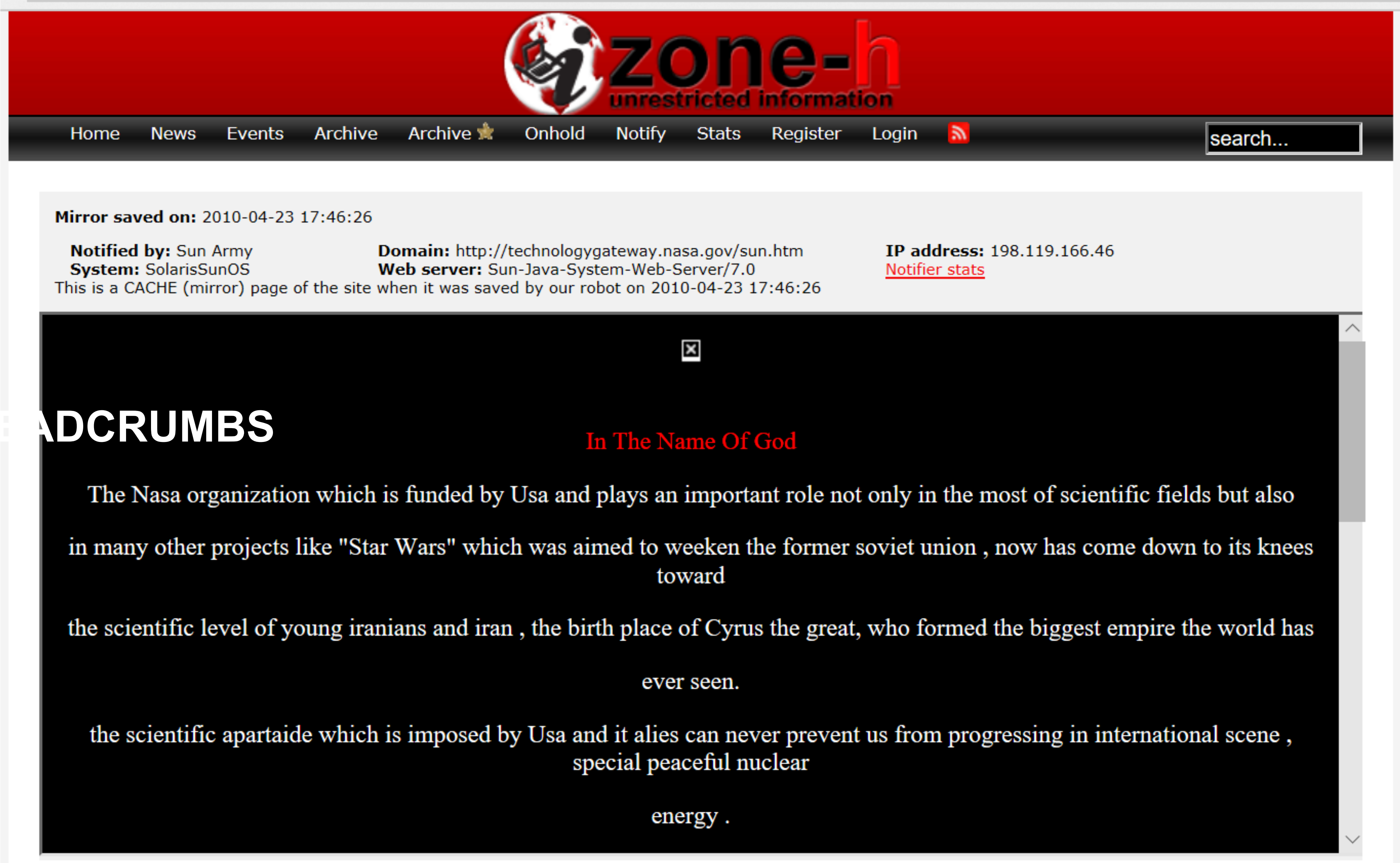
Amin Shokohi

Mohammad Sadegh Ahmadzadegan

Omid Ghaffarinia

Sina Keissar

Nader Saedi



Mirror saved on: 2010-04-23 17:46:26

Notified by: Sun Army
System: SolarisSunOS
Domain: http://technologygateway.nasa.gov/sun.htm
Web server: Sun-Java-System-Web-Server/7.0
IP address: 198.119.166.46
Notifier stats

This is a CACHE (mirror) page of the site when it was saved by our robot on 2010-04-23 17:46:26

ADCRUMBS

In The Name Of God

The Nasa organization which is funded by Usa and plays an important role not only in the most of scientific fields but also

in many other projects like "Star Wars" which was aimed to weeken the former soviet union , now has come down to its knees toward

the scientific level of young iranians and iran , the birth place of Cyrus the great, who formed the biggest empire the world has

ever seen.

the scientific apartaide which is imposed by Usa and it alies can never prevent us from progressing in international scene , special peaceful nuclear

energy .

Iranian Org Structure (Maurer 2018)

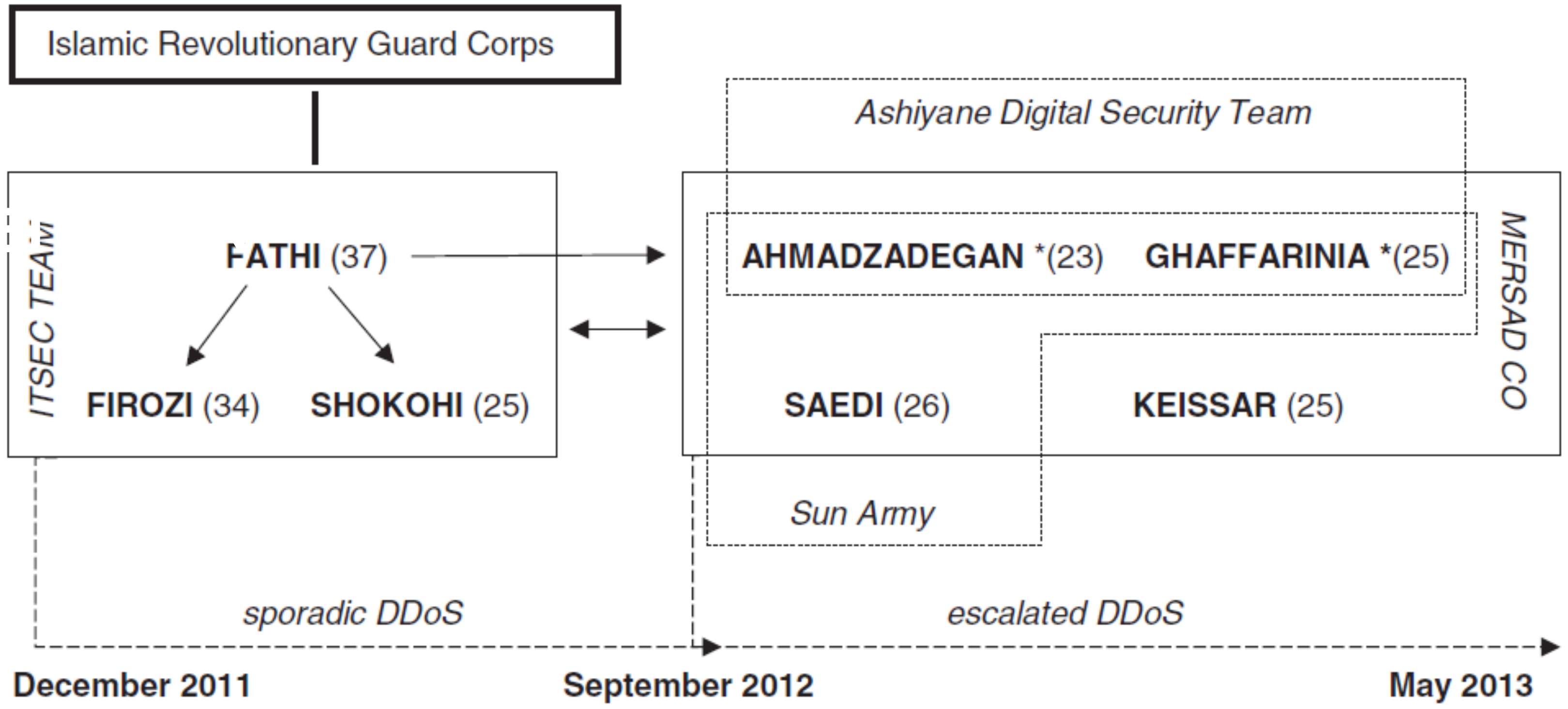
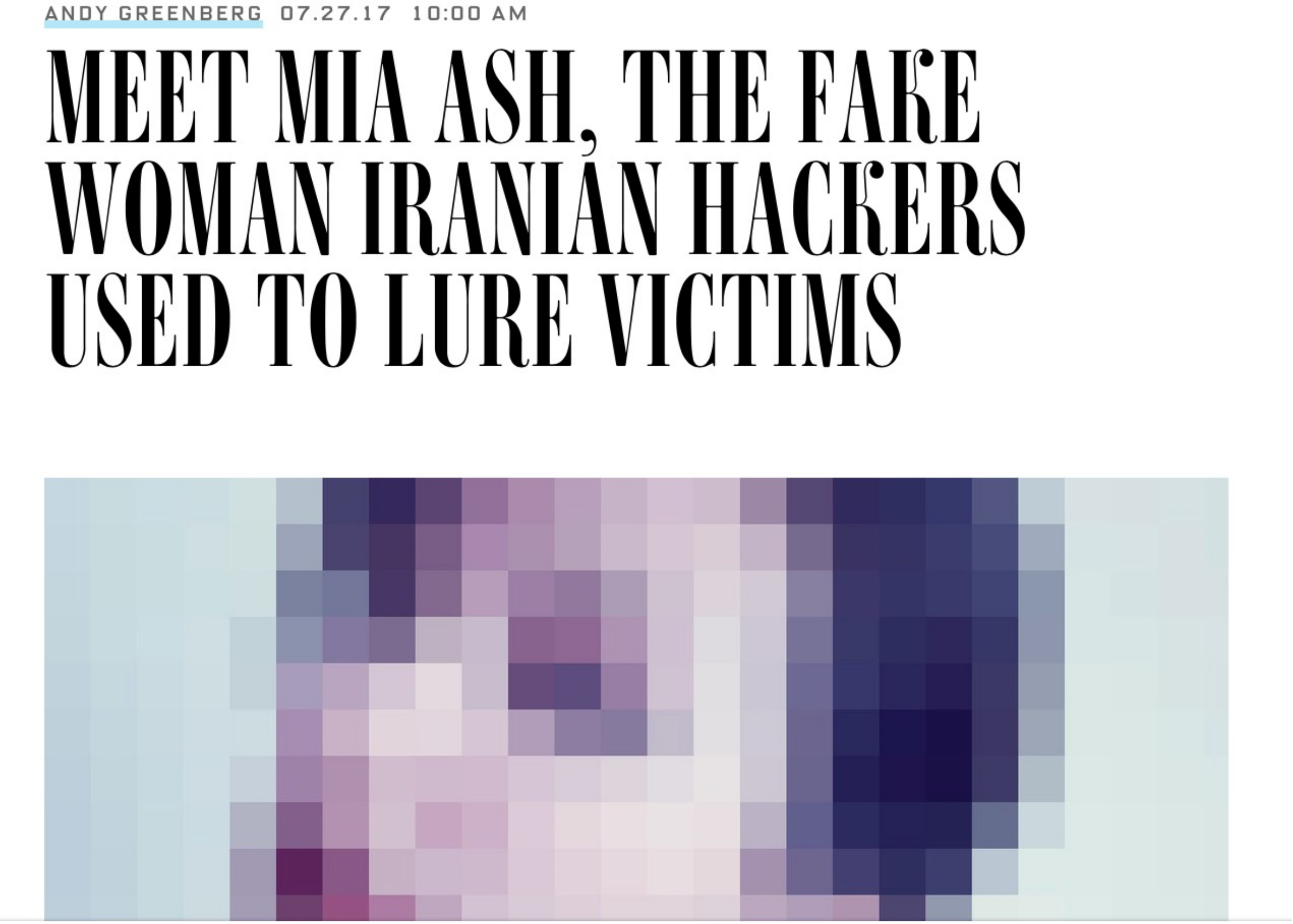


FIGURE 5.1 Organizational structure and timeline of hackers mentioned in US indictment in 2016 of seven Iranian hackers.

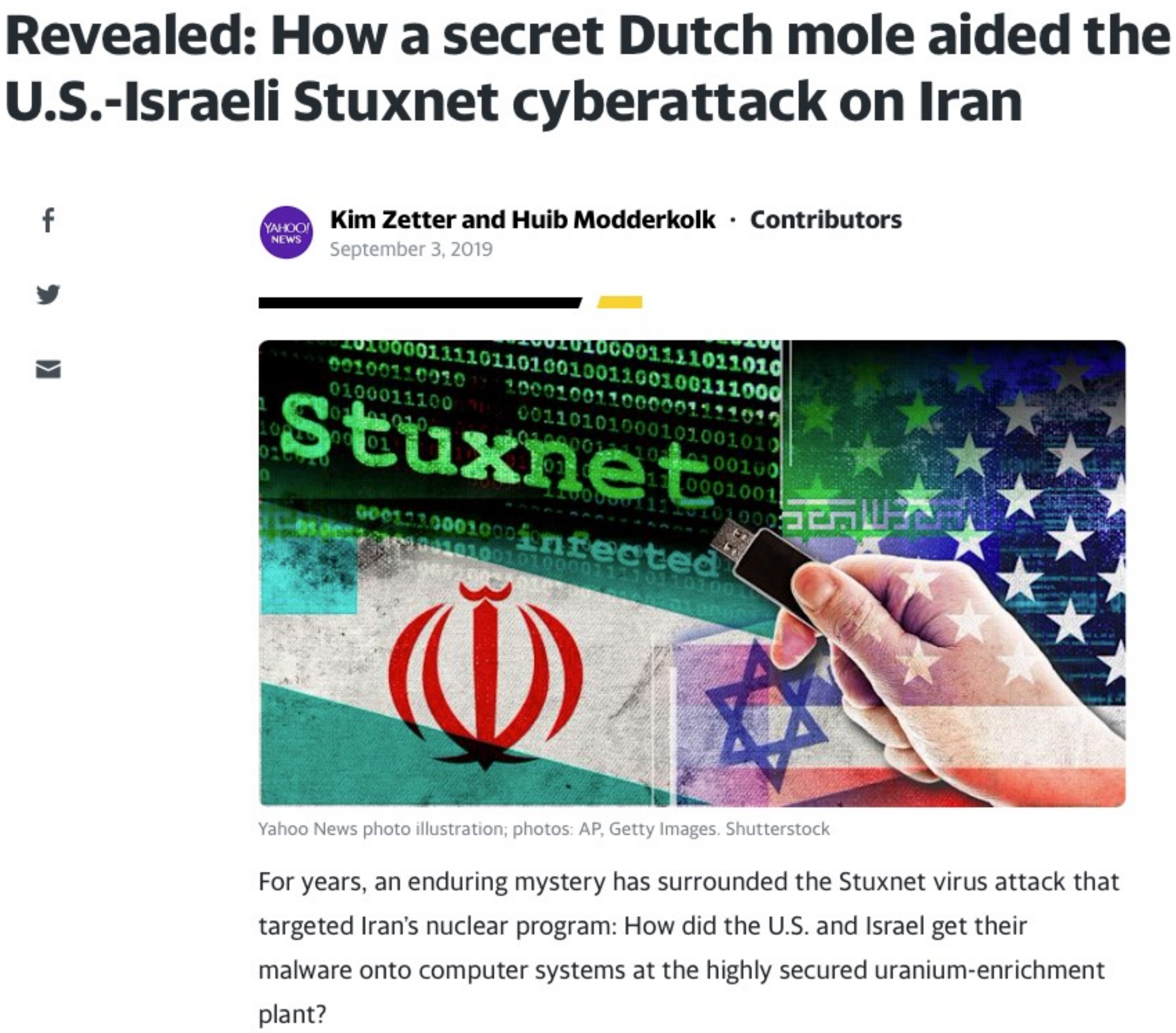
Linkedin Used by Iranians (Wired & Secureworks 2017)



ANDY GREENBERG 07.27.17 10:00 AM

MEET MIA ASH, THE FAKE WOMAN IRANIAN HACKERS USED TO LURE VICTIMS

Others



Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran

Kim Zetter and Huib Modderkolk · Contributors
September 3, 2019

Yahoo News photo illustration; photos: AP, Getty Images. Shutterstock

For years, an enduring mystery has surrounded the Stuxnet virus attack that targeted Iran's nuclear program: How did the U.S. and Israel get their malware onto computer systems at the highly secured uranium-enrichment plant?

Conclusion

- All major states have offensive cyber capability these are just some examples
- Cyber is currently just short of war so a good option for nation states
- Attacks can be mounted by militray or intelligence operations, private partners, co-opt organised crime and patritoc hackers
- Nations are also integrating cyber attacks in their war plans

Thank you for your attention

NHL STENDEN

university of applied sciences