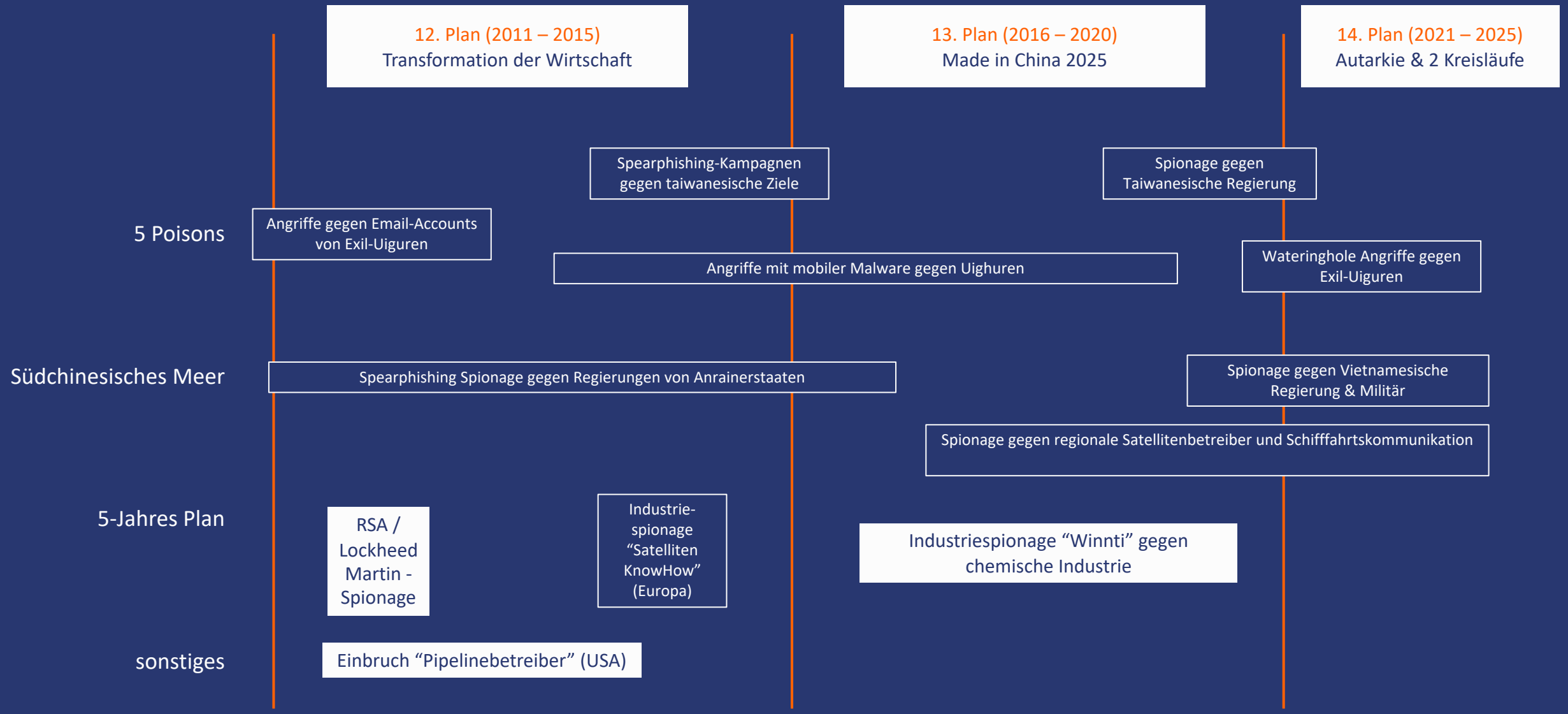
Real World Cyber
strategische Ziele und ihre Auswirkungenim Cyberraum

Nov 2022, Dror-John Röcher, intcube GmbH


Barents Sea
Kara Sea
SWEDEN
FINLAND
ESTONIA
RUSSIA
KAZAKHSTAN
MONGOLIA
UZBEKISTAN
TURKMENISTAN
CHINA
IRAN
IRAQ
AFGHANISTAN
PAKISTAN
INDIA
SAUDI ARABIA
KUWAIT
U.A.E.
OMAN
YEMEN
Red Sea
Arabian Sea
Bay of Bengal
ERITREA
SUDAN
SOMALIA
ETHIOPIA
SOUTH SUDAN
CENTRAL AFRICAN REP.
KENYA
UGANDA
GABON
CONGO
TANZANIA
SRI LANKA
MALDIVES
SEYCHELLES
MYANMAR
VIETNAM
CAMBODIA
LAOS
BRUNEI
MALAYSIA
South China Sea
INDIAN OCEAN


12. Plan (2011 – 2015)
Transformation der Wirtschaft
13. Plan (2016 – 2020)
Made in China 2025
14. Plan (2021 – 2025)
Autarkie & 2 Kreisläufe
5 Poisons
Südchinesisches Meer
5-Jahres Plan
sonstiges
Angriffe gegen Email-Accounts von Exil-Uiguren
Spearphishing-Kampagnen gegen taiwanesische Ziele
Spionage gegen Taiwanesische Regierung
Angriffe mit mobiler Malware gegen Uighuren
Wateringhole Angriffe gegen Exil-Uiguren
Spearphishing Spionage gegen Regierungen von Anrainerstaaten
Spionage gegen Vietnamesische Regierung & Militär
Spionage gegen regionale Satellitenbetreiber und Schifffahrtskommunikation
RSA / Lockheed Martin - Spionage
Industrie-spionage “Satelliten KnowHow” (Europa)
Industriespionage “Winnti” gegen chemische Industrie
Einbruch “Pipelinebetreiber” (USA)

Dienst der Außenaufklärung der Russischen Föderation (SVR)

Служба внешней разведки Российской Федерации

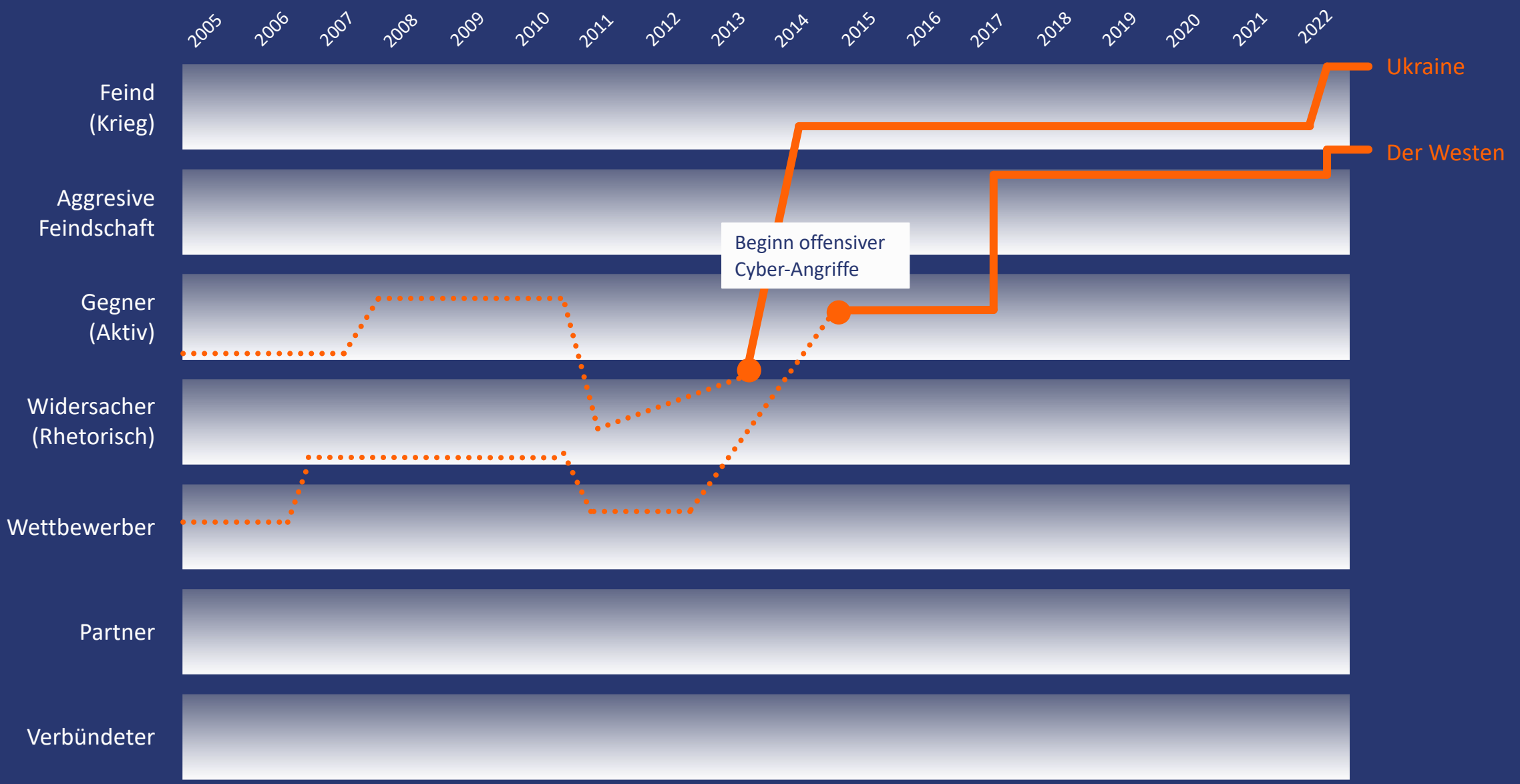
Föderaler Dienst für Sicherheit der Russischen Föderation (FSB)

Федеральная служба безопасности Российской Федерации

Hauptverwaltung für Aufklärung (GRU)

Главное разведывательное управление

Politische Haltung der Russischen Regierung



basierend auf “International Institute for Strategic Studies” (https://www.iiss.org/)

Russische Cyber-Angriffe gegen die Ukraine März 2013 – Juli 2021

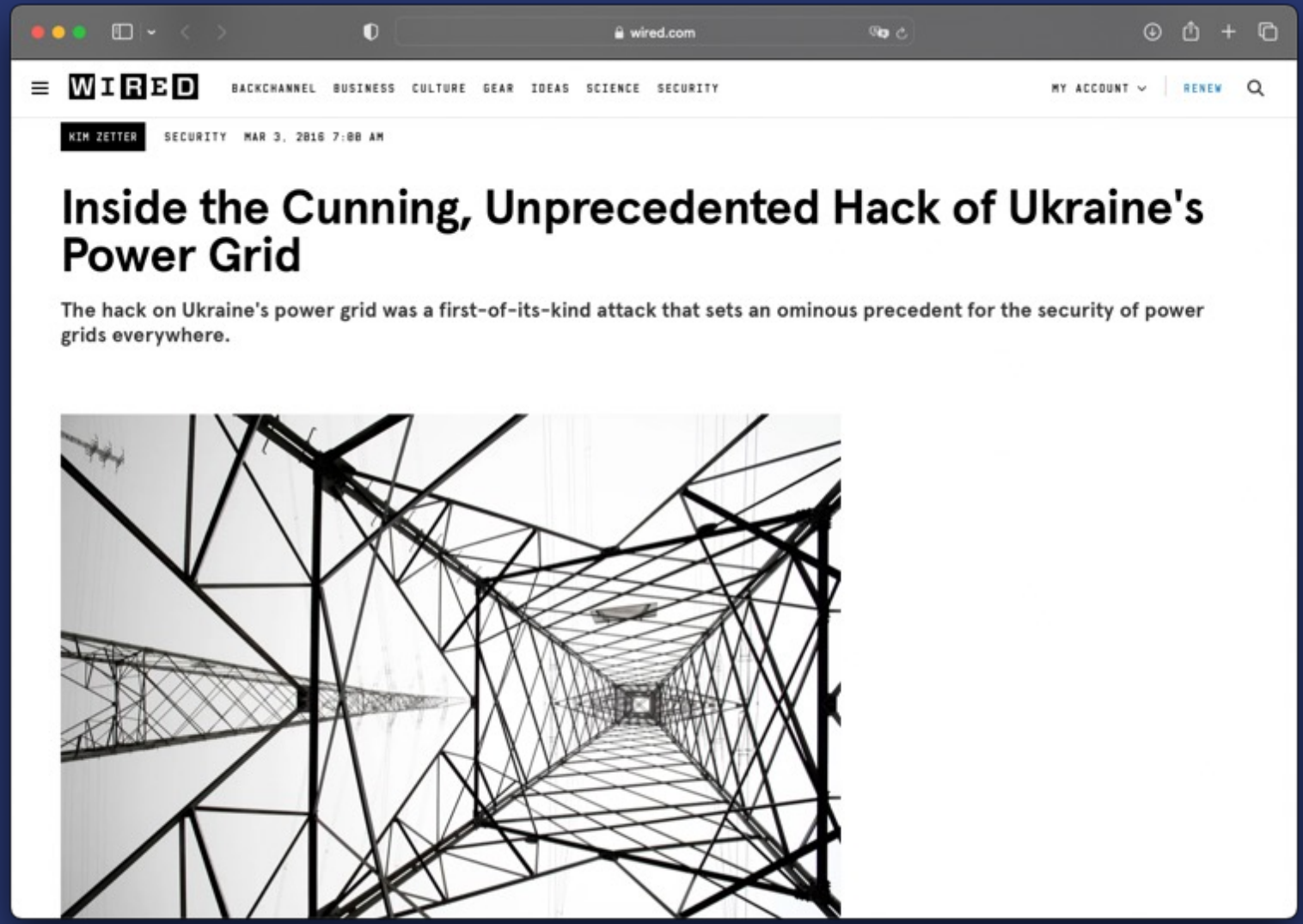
Mid-2013	Ukrainian-government, law-enforcement and military officials | harassment operation disguised as espionage | interference in discussions about the EU–Ukraine Association Agreement
Mar 2014	Crimea's telecommunications infrastructure, major Ukrainian websites, and mobile phones of key Ukrainian officials | disabling attacks | preparation for annexation of Crimea
May 2014	Ukraine's Central Election Commission (CEC) | harassment and disruption | support for Russia's preferred presidential candidate
Dec 2014–16	Ukrainian artillery units | malware implant on Android devices | intelligence collection to enable strikes against the units in support of pro-Russian separatists in eastern Ukraine
2014	Ukrainian public | disinformation regarding the Russian annexation of Crimea and anti-Semitic incidents in Ukraine | to legitimise Russia's annexation of Crimea and build support for the Russian military in the subsequent conflict in eastern Ukraine
2014–Nov 2021	Ukrainian state entities and critical infrastructure (targeted 1,500 government computer systems) | developed custom malware 'Pterodo' | to gain control over Ukraine's critical-infrastructure facilities, conduct espionage, informational and psychological influence and block access to information systems
Dec 2015	Three Ukrainian energy-distribution companies | disruption | to sabotage the supply of electricity to more than 225,000 Ukrainian customers
Apr 2016	Energy company | initial penetration | preparation for sabotage attack in December 2016
Oct 2016	Ministry of Finance and State Treasury Service | initial penetration | preparation for later sabotage attack
Dec 2016	Companies supporting Ukraine's electricity grid and Ministry of Finance and State Treasury Service | deployment of destructive malware | sabotage (Ukraine reported 6,500 cyber attacks against five government agencies and 31 state information resources in the previous two months)
Jun 2017	Ukrainian banks and corporations, including the state power distributor | 'NotPetya' ransomware | disabling attacks (the attack caused serious damage and disruption worldwide)
Oct 2017	Kyiv's metro system and Odessa airport | 'BadRabbit' ransomware | to disable and disrupt
Autumn 2017	Ukrainian government agencies, local government bodies, state-owned critical infrastructure | ransomware | to disable and disrupt
Jun 2018	Ukrainian companies, banks and energy infrastructure | create backdoors | preparation for a large-scale attack
Jul 2018	Ukraine's Aul Chlorine Overflow station (sewerage and water purification) | 'VPNFilter' malware | social disruption and damage
Nov 2018	Ukrainian government and military targets | malware and disinformation | planning and execution of Russia's seizure of Ukrainian vessels and crew on 25 November 2018 (Kerch Strait crisis)
24–25 Feb 2019	CEC | distributed denial-of-service (DDoS) attack | to sabotage the election outcome
Mar 2019	CEC | phishing | to disrupt election declarations (attacks were foiled)
Oct–Nov 2019	Ukrainian diplomats, government officials, journalists, law-enforcement officials, military officials and non-governmental organisations (NGOs) | spear-phishing campaign | espionage
Feb 2020	Ukrainian national-security institutions, such as the Hetman Petro Sahaidachnyi National Ground Forces Academy | spear-phishing campaign | espionage
Feb 2020	Ukrainian citizens | phishing to modify or destroy data, and disinformation relating to the coronavirus pandemic | social disruption (outcome included violent protests and clashes with the police)
May 2020	Ukrainian citizens | social-influencing operations and disinformation | to create panic and confusion amid the coronavirus pandemic and by raising the spectre of creation of the 'Republic of Novorossiya'
Aug 2020	Ukrainian public agencies and critical infrastructure | malware | disruption and sabotage on the eve of Ukraine's Independence Day
Jan 2021	Ukrainian state institutions | phishing email | reconnaissance, possible disruption
Jan–Mar 2021	Ukrainian government officials | massive and sustained malware attacks in unprecedented numbers | strategic disruption (attacks were unsuccessful but coincided with the build-up of Russian forces on the border with Ukraine)
Feb 2021	Ukrainian security and defence websites, other state institutions and strategic enterprises | large-scale DDoS attacks | sabotage (a new form of attack that rendered the websites inaccessible even after the end of the attacks)
Feb 2021	File-sharing system used by Ukrainian government agencies | uploaded malicious documents containing macro scripts | espionage
Mar 2021	Ukrainian government information resources | penetration operations | possible control of state information resources
Jun 2021	Ukrainian government and private sector | spear-phishing operation | espionage
Jul 2021	Ukrainian Naval Forces website | malware and publishing fake documents | to express discontent regarding the *Sea Breeze* 2021 military exercise involving Black Sea nations and NATO allies and partners and to spread disinformation about the military drill

Russische Cyber-Angriffe gegen die Ukraine März 2013 – Juli 2021

Legende

- KRITIS
- Regierung
- InfoOp
- Militär

2015


wired.com
WIRED
BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY
MY ACCOUNT
RENEW
KIM ZETTER
SECURITY MAR 3, 2016 7:00 AM
Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid
The hack on Ukraine's power grid was a first-of-its-kind attack that sets an ominous precedent for the security of power grids everywhere.

2016 - 2017


wired.com
WIRED
BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY
MY ACCOUNT
RENEW
ANDY GREENBERG
EXCERPT
SECURITY AUG 22, 2018 5:00 AM
The Untold Story of NotPetya, the Most Devastating Cyberattack in History
Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.
00 20 00 2F 00 53 00 54 00 30 20 00
00 64 00 3A 00 25 00 30 00 00 32
00 74 00 20 00 25 36 00 30
00 30 00 32 00 64 2E 00 20
00 00 00 73 00 60 00 70 00 52 74 00
00 6E 00 2E 00 65 00 70 00 79 65 00
MIKE MCQUADE

"All the News That's Fit to Print"

The New York Times

Late Edition

Today, cloudy, rain, snow and ice north and west, clearing later, high 38. Tonight, mostly clear, colder, low 22. Tomorrow, mostly sunny, cold, high 34. Weather map, Page B10.

VOL. CLXXI ... No. 59,345 NEW YORK, FRIDAY, FEBRUARY 25, 2022 $3.00

WAR IN UKRAINE

RUSSIANS PUSH INTO OUTSKIRTS OF CAPITAL AS DEATHS RISE AND THOUSANDS FLEE WEST

EVGENIY MALOLETKA/ASSOCIATED PRESS

DESTRUCTION A military facility in southern Ukraine on Thursday as Russian forces unleashed artillery strikes across the nation.

Big Explosion Is Seen Over Kyiv; Zelensky Says He's 'Target No. 1'

This article is by ***Michael Schwirtz****,* ***Eric Schmitt*** *and* ***Neil MacFarquhar****.*

SLOVYANSK, Ukraine — Russia continued its attack on Ukraine early Friday, one day after it invaded the country by land, sea and air, killing more than 100 Ukrainian soldiers and civilians and ominously touching off a pitched battle at the highly radioactive area around the Chernobyl nuclear reactor that melted down in 1986.

Videos verified by The New York Times showed a large explosion in the sky over the outskirts of southern Kyiv, the capital, around 4:20 a.m. Friday. Witnesses filmed fiery debris falling over parts of the city, and videos appeared to show at least two surface-to-air missiles being fired from Kyiv before the explosion.

On Thursday, Day 1 of the first major land war in Europe in decades, the Russian military began its attack before sunrise with the terrifying thud of artillery strikes on airports and military installations all over Ukraine. A senior Pentagon official said that three lines of Russian troops and military forces were moving swiftly toward Ukrainian cities — one heading south from Belarus toward Kyiv; another toward Kharkiv, in northeast Ukraine; and a third toward Kherson in the south, near Crimea. The forces were using missiles and long-range artillery, the official said.

By Thursday's end, Russian

Continued on Page A6

SARAHBETH MANEY/THE NEW YORK TIMES

President Biden denounced a "brutal assault" and said that "America stands up to bullies."

wired.com

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY MY ACCOUNT RENEW

MATT BURGESS SECURITY MAR 23, 2022 7:00 AM

A Mysterious Satellite Hack Has Victims Far Beyond Ukraine

The biggest hack since Russia's war began knocked thousands of people offline. The spillover extends deep into Europe.

PHOTOGRAPH: BJDLZX/GETTY IMAGES

Add page to Reading List

Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says

Zero Day Gift a subscription

Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says

Contrary to initial reports that it resulted in a "really huge loss in communications in the very beginning of war," the hack did not have a huge impact on ability to coordinate military operations.

Kim Zetter
Sep 26

12

In the early weeks of the war in Ukraine, the public learned about a hack that targeted modems used for Viasat internet connectivity on the day the invasion began in February.

The hack occurred on Feb. 24 between 5am and 9 am, around the same time that Russian forces began their onslaught of Ukraine with missiles, and Russian troops began moving into the country.

query.prod.cms.rt.microsoft.com

Microsoft

Defending Ukraine: Early Lessons from the Cyber War

lieber.westpoint.edu

UKRAINE SYMPOSIUM – U.S. OFFENSIVE CYBER OPERATIONS IN SUPPORT OF UKRAINE

by Michael N. Schmitt | Jun 6, 2022

Last Wednesday, General Paul Nakasone, Commander of United States Cyber Command and Director of the National Security Agency, opened the NATO Cooperative Cyber Defense Centre of Excellence's annual CyCon Conference. In his address, General Nakasone discussed the "defend forward" and "persistent engagement" operational concepts set forth,

SUBSCRIBE

SEARCH POSTS

RELATED POSTS

Symposium Intro: Ukraine-Russia Armed Conflict

by Sean Watts, Winston Williams, Ronald Alcala

February 28, 2022

Russia's "Special Military Operation" and the (Claimed) Right of Self-Defense

by Michael N. Schmitt

February 28, 2022

Legal Status of Ukraine's Resistance Forces


4
5

Fragen & Antworten

Broschüre

https://intcube.io/publications

Kontakt

https://linkedin.com/in/droecher