Burrowing Through The Network: *Contextualizing The Vulkan Leaks & State-Sponsored Offensive Operations*

Joe Slowik, Paralus LLC

Quick Background

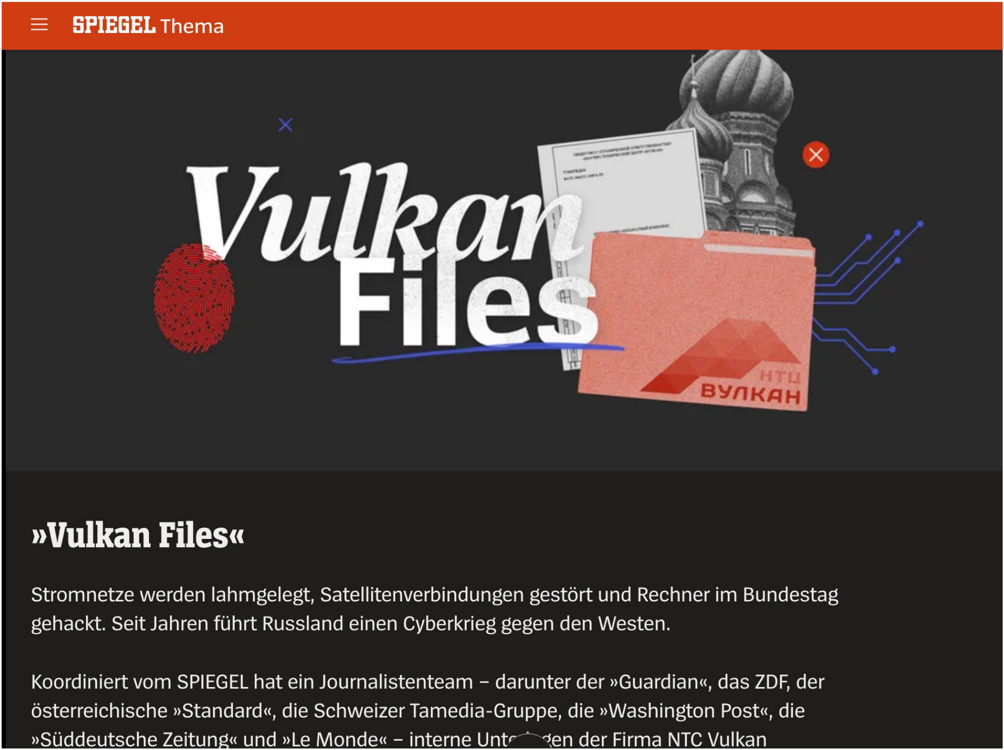
- *Current:*
    - *CTI & ICS/OT Consulting @ Paralus LLC*
    - *Threat Intelligence Management @ Huntress*
- *Previous:*
    - *Threat Intelligence & Detection Engineering Lead @ Gigamon*
    - *Threat Research @ DomainTools & Dragos*
    - *Incident Response Lead @ Los Alamos National Laboratory*
    - *“Various” @ US Navy*

Agenda

- The Vulkan Files
- Vulkan & Russian Cyber Operations
- Orienting Vulkan Capabilities In Cyber History
- Future Of Offensive Cyber Operations
- Conclusions

The Vulkan Files

What Are The Vulkan Files?



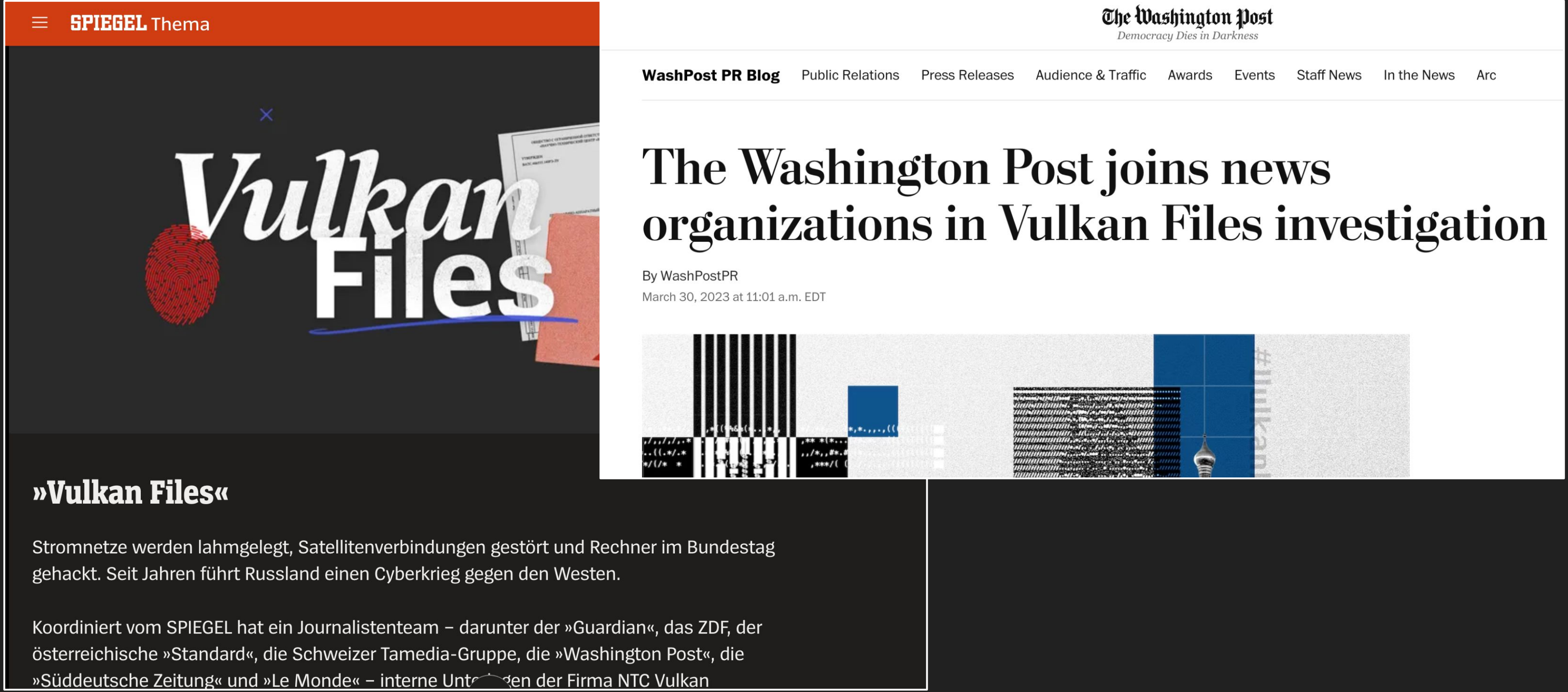
SPIEGEL Thema

»Vulkan Files«

Stromnetze werden lahmgelegt, Satellitenverbindungen gestört und Rechner im Bundestag gehackt. Seit Jahren führt Russland einen Cyberkrieg gegen den Westen.

Koordiniert vom SPIEGEL hat ein Journalistenteam – darunter der »Guardian«, das ZDF, der österreichische »Standard«, die Schweizer Tamedia-Gruppe, die »Washington Post«, die »Süddeutsche Zeitung« und »Le Monde« – interne Unterlagen der Firma NTC Vulkan

What Are The Vulkan Files?



»Vulkan Files«

Stromnetze werden lahmgelegt, Satellitenverbindungen gestört und Rechner im Bundestag gehackt. Seit Jahren führt Russland einen Cyberkrieg gegen den Westen.

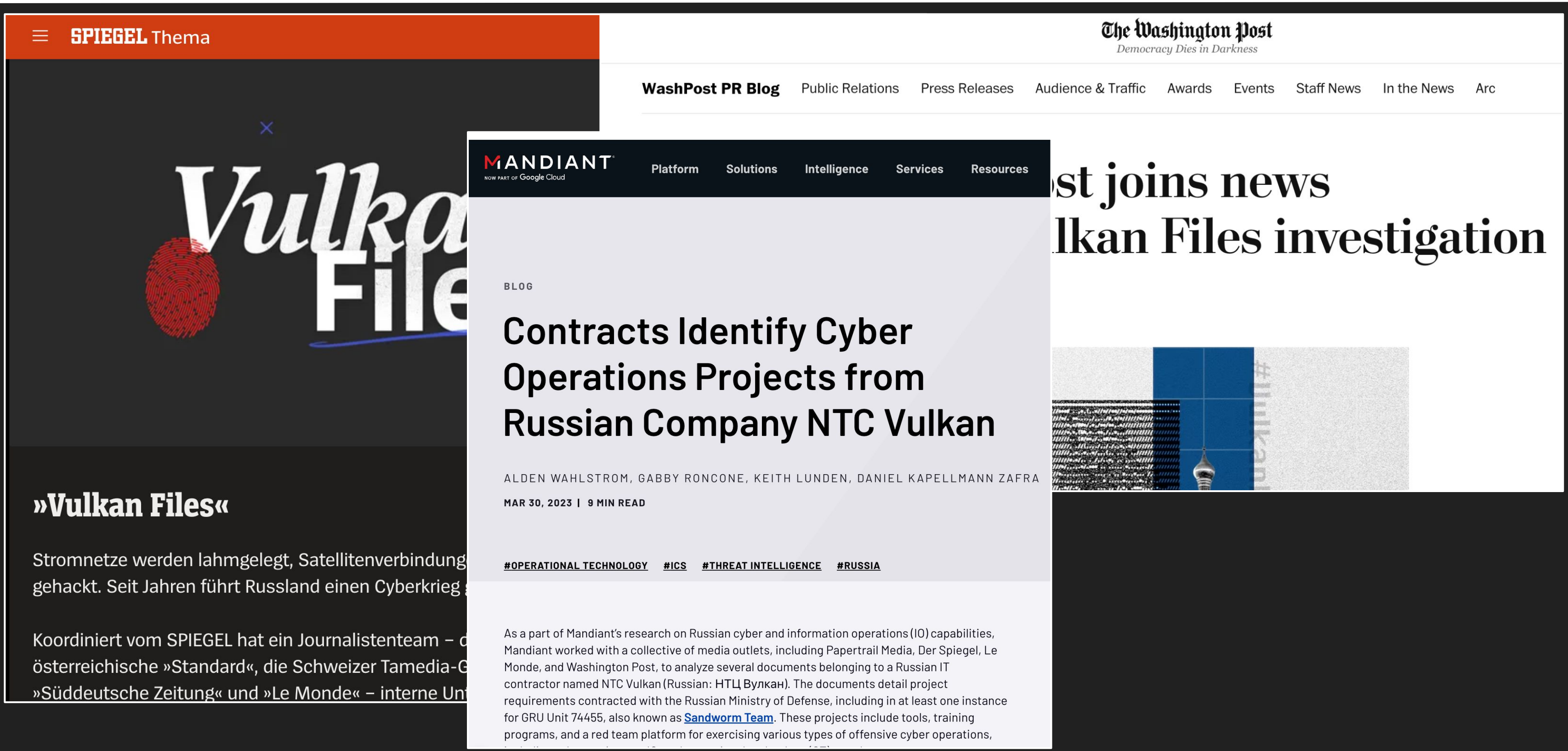
Koordiniert vom SPIEGEL hat ein Journalistenteam – darunter der »Guardian«, das ZDF, der österreichische »Standard«, die Schweizer Tamedia-Gruppe, die »Washington Post«, die »Süddeutsche Zeitung« und »Le Monde« – interne Unterlagen der Firma NTC Vulkan

The Washington Post joins news organizations in Vulkan Files investigation

By WashPostPR

March 30, 2023 at 11:01 a.m. EDT

What Are The Vulkan Files?



»Vulkan Files«

Stromnetze werden lahmgelegt, Satellitenverbindung
gehackt. Seit Jahren führt Russland einen Cyberkrieg

Koordiniert vom SPIEGEL hat ein Journalistenteam – d
österreichische »Standard«, die Schweizer Tamedia-G
»Süddeutsche Zeitung« und »Le Monde« – interne Un

st joins news
lkan Files investigation

BLOG

Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan

ALDEN WAHLSTROM, GABBY RONCONE, KEITH LUNDEN, DANIEL KAPELLMANN ZAFRA

MAR 30, 2023 | 9 MIN READ

#OPERATIONAL TECHNOLOGY #ICS #THREAT INTELLIGENCE #RUSSIA

As a part of Mandiant's research on Russian cyber and information operations (IO) capabilities, Mandiant worked with a collective of media outlets, including Papertrail Media, Der Spiegel, Le Monde, and Washington Post, to analyze several documents belonging to a Russian IT contractor named NTC Vulkan (Russian: НТЦ Вулкан). The documents detail project requirements contracted with the Russian Ministry of Defense, including in at least one instance for GRU Unit 74455, also known as Sandworm Team. These projects include tools, training programs, and a red team platform for exercising various types of offensive cyber operations,

What Are The Vulkan Files?

What Are The Vulkan Files?

NTC Vulkan

Computer Technology Firm, Founded In 2010 By Russian Military Veterans With Approval To Perform Classified Work.

What Are The Vulkan Files?

NTC Vulkan

Computer Technology Firm, Founded In 2010 By Russian Military Veterans With Approval To Perform Classified Work.

The Leaks

Unknown Entity Leaked Project Information And Documentation For Various Projects To German Journalists

What Are The Vulkan Files?

NTC Vulkan

Computer Technology Firm, Founded In 2010 By Russian Military Veterans With Approval To Perform Classified Work.

The Leaks

Unknown Entity Leaked Project Information And Documentation For Various Projects To German Journalists

The Significance

Rarely Do We See The “Nuts & Bolts” Of CNO Tool Development & Procurement Processes - Lots Of Data To Go Through!

NTC Vulkan

Programs Of Interest

Programs Of Interest

Scan-V

Programs Of Interest

Scan-V

Amesit

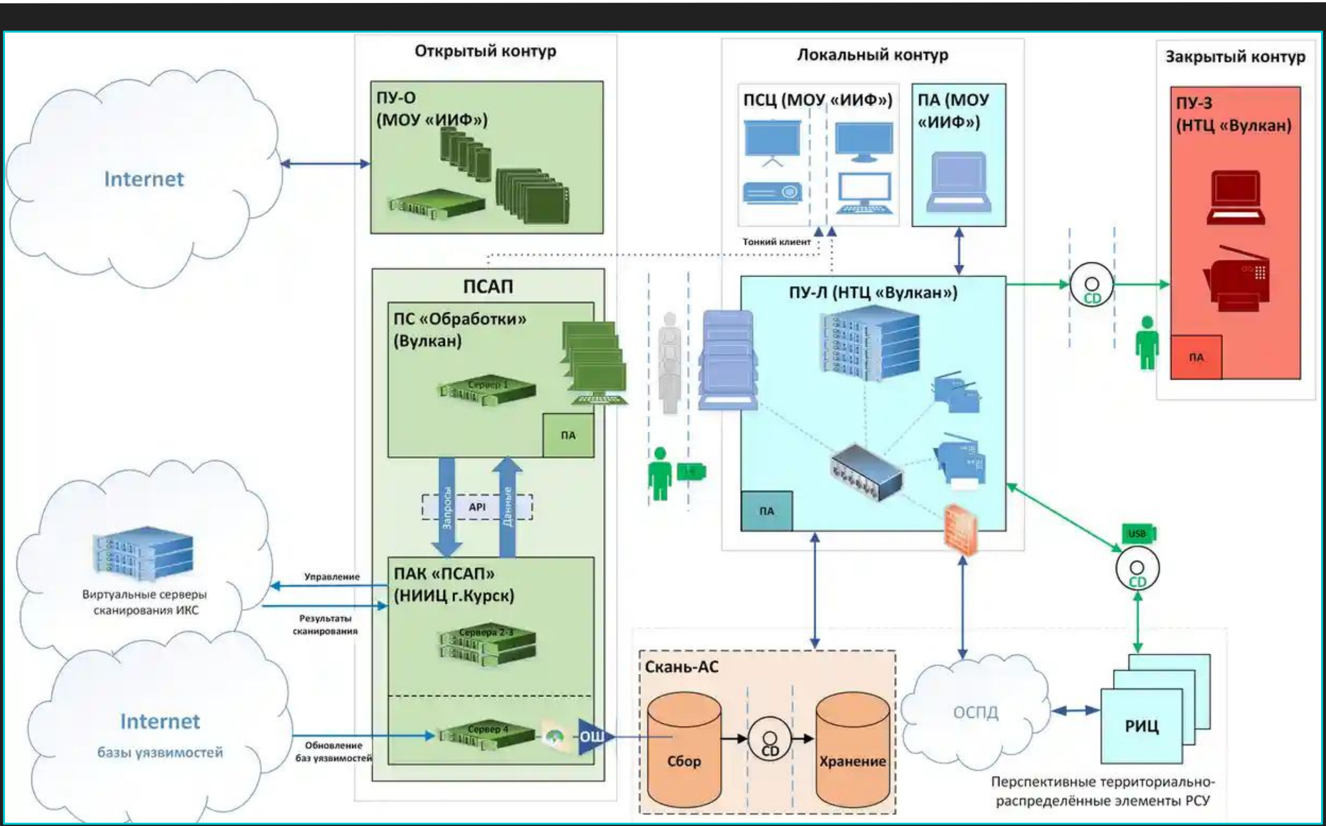
Programs Of Interest

Scan-V

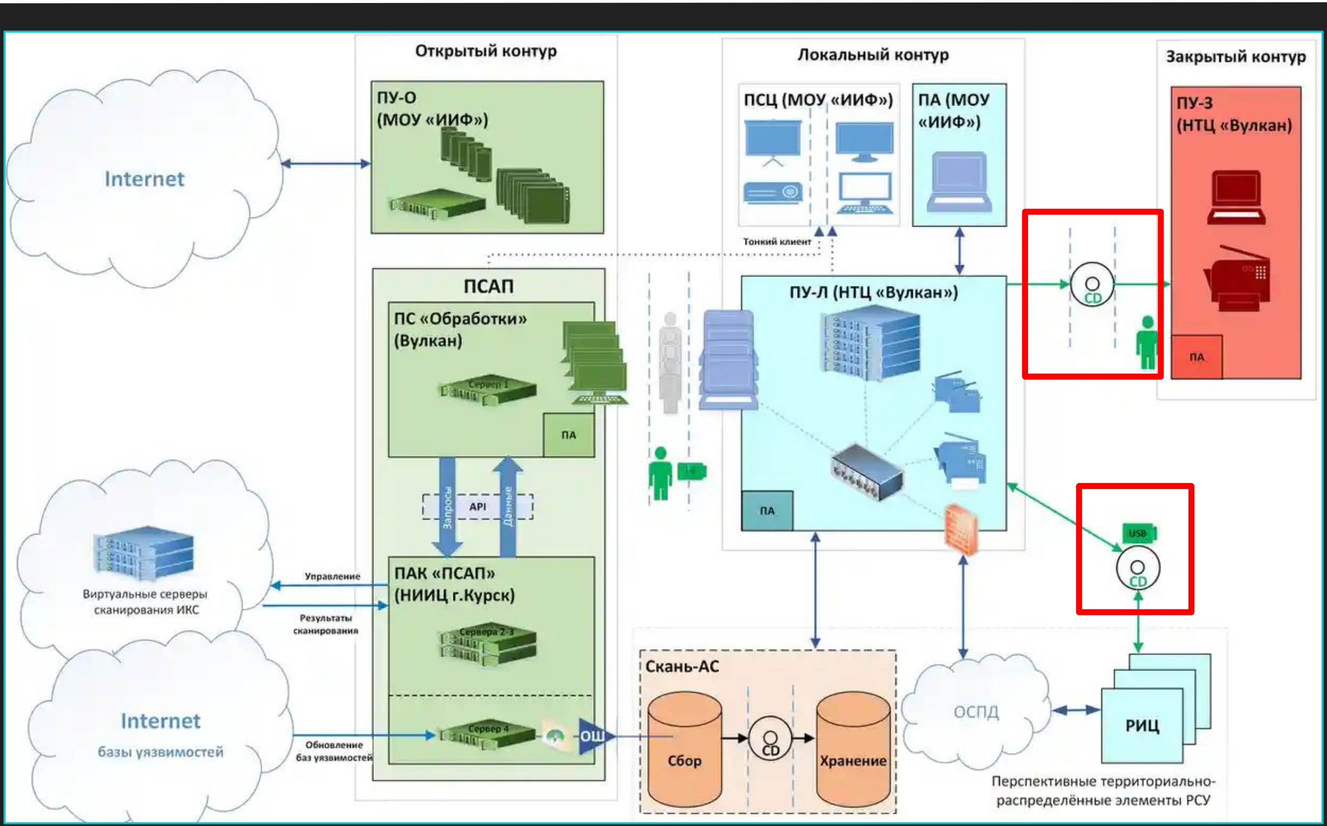
Amesit

Krystal-2V

Scan-V


Открытый контур
Локальный контур
Закрытый контур
Internet
ПУ-О
(МОУ «ИИФ»)
ПСЦ (МОУ «ИИФ»)
ПА (МОУ «ИИФ»)
ПУ-З
(НТЦ «Вулкан»)
Тонкий клиент
ПСАП
ПС «Обработки»
(Вулкан)
Сервер 1
ПА
Запросы
API
Данные
ПУ-Л (НТЦ «Вулкан»)
ПА
CD
ПА
USB
CD
Виртуальные серверы
сканирования ИКС
Управление
Результаты
сканирования
ПАК «ПСАП»
(НИИЦ г.Курск)
Сервера 2-3
Internet
базы уязвимостей
Обновление
баз уязвимостей
Сервер 4
ОШ
Скань-АС
Сбор
CD
Хранение
ОСПД
РИЦ
Перспективные территориально-
распределённые элементы РСУ

Scan-V


Открытый контур
Локальный контур
Закрытый контур
Internet
ПУ-О
(МОУ «ИИФ»)
ПСЦ (МОУ «ИИФ»)
ПА (МОУ
«ИИФ»)
ПУ-З
(НТЦ «Вулкан»)
ПА
Тонкий клиент
ПСАП
ПС «Обработки»
(Вулкан)
Сервер 1
ПА
ПУ-Л (НТЦ «Вулкан»)
CD
ПА
API
Запросы
Данные
USB
CD
Виртуальные серверы
сканирования ИКС
Управление
Результаты
сканирования
ПАК «ПСАП»
(НИИЦ г.Курск)
Сервера 2-3
Сервер 4
ОШ
Internet
базы уязвимостей
Обновление
баз уязвимостей
Скань-АС
Сбор
CD
Хранение
ОСПД
РИЦ
Перспективные территориально-
распределённые элементы РСУ

Scan-V

Scan-V

Design

Scan-V

Design

- Distributed, Multi-Component System Crossing Various Information Boundaries
- Designed For Automated Tasking & Action Within Pre-Programmed Capabilities

Scan-V

Design

- Distributed, Multi-Component System Crossing Various Information Boundaries
- Designed For Automated Tasking & Action Within Pre-Programmed Capabilities

Purpose

Scan-V

Design

- Distributed, Multi-Component System Crossing Various Information Boundaries
- Designed For Automated Tasking & Action Within Pre-Programmed Capabilities

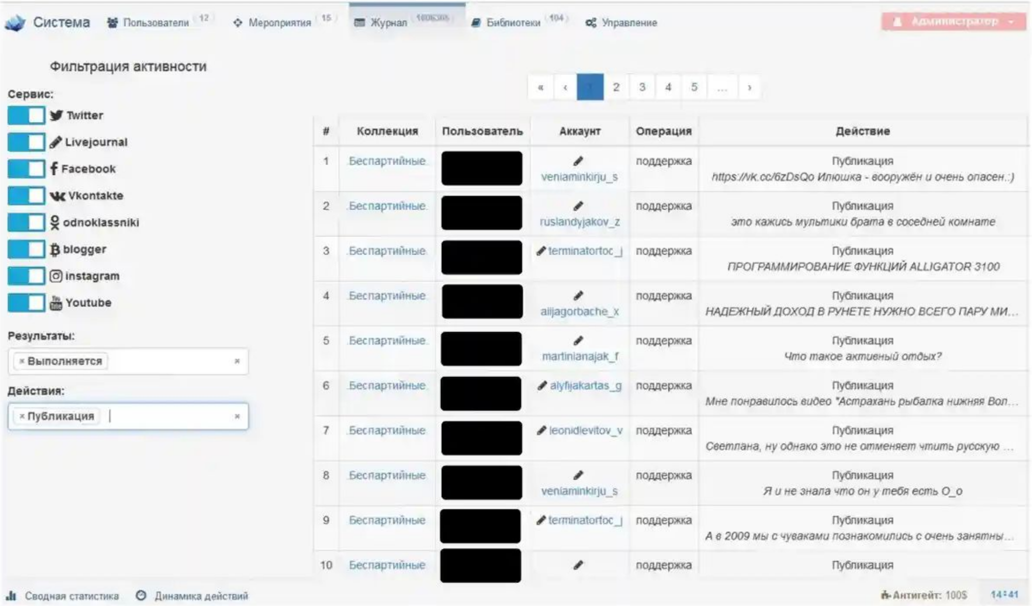
Purpose

- Combine External Scanning Functionality With Catalog Of Vulnerabilities & Exploits
- Automate Or Increase The Efficiency Of Cyber Operations, Infrastructure Harvesting

Amesit

28

[redacted]



Фильтрация активности

Сервис:

- Twitter
- Livejournal
- Facebook
- Vkontakte
- odnoklassniki
- blogger
- instagram
- Youtube

Результаты: × Выполняется

Действия: × Публикация

#	Коллекция	Пользователь	Аккаунт	Операция	Действие
1	Беспартийные	[redacted]	veniaminkirju_s	поддержка	Публикация *https://vk.cc/6zDsQo Илюшка - вооружён и очень опасен.:)*
2	Беспартийные	[redacted]	ruslandyjakov_z	поддержка	Публикация *это кажись мультики брата в соседней комнате*
3	Беспартийные	[redacted]	terminatortoc_j	поддержка	Публикация *ПРОГРАММИРОВАНИЕ ФУНКЦИЙ ALLIGATOR 3100*
4	Беспартийные	[redacted]	aiijagorbache_x	поддержка	Публикация *НАДЕЖНЫЙ ДОХОД В РУНЕТЕ НУЖНО ВСЕГО ПАРУ МИ…*
5	Беспартийные	[redacted]	martinianajak_f	поддержка	Публикация *Что такое активный отдых?*
6	Беспартийные	[redacted]	alyfijakartas_g	поддержка	Публикация *Мне понравилось видео "Астрахань рыбалка нижняя Вол…*
7	Беспартийные	[redacted]	leonidlevitov_v	поддержка	Публикация *Светлана, ну однако это не отменяет чтить русскую …*
8	Беспартийные	[redacted]	veniaminkirju_s	поддержка	Публикация *Я и не знала что он у тебя есть О_о*
9	Беспартийные	[redacted]	terminatortoc_j	поддержка	Публикация *А в 2009 мы с чуваками познакомились с очень занятны…*
10	Беспартийные	[redacted]		поддержка	Публикация

Рисунок 22 – Раздел «Журнал»

Amesit

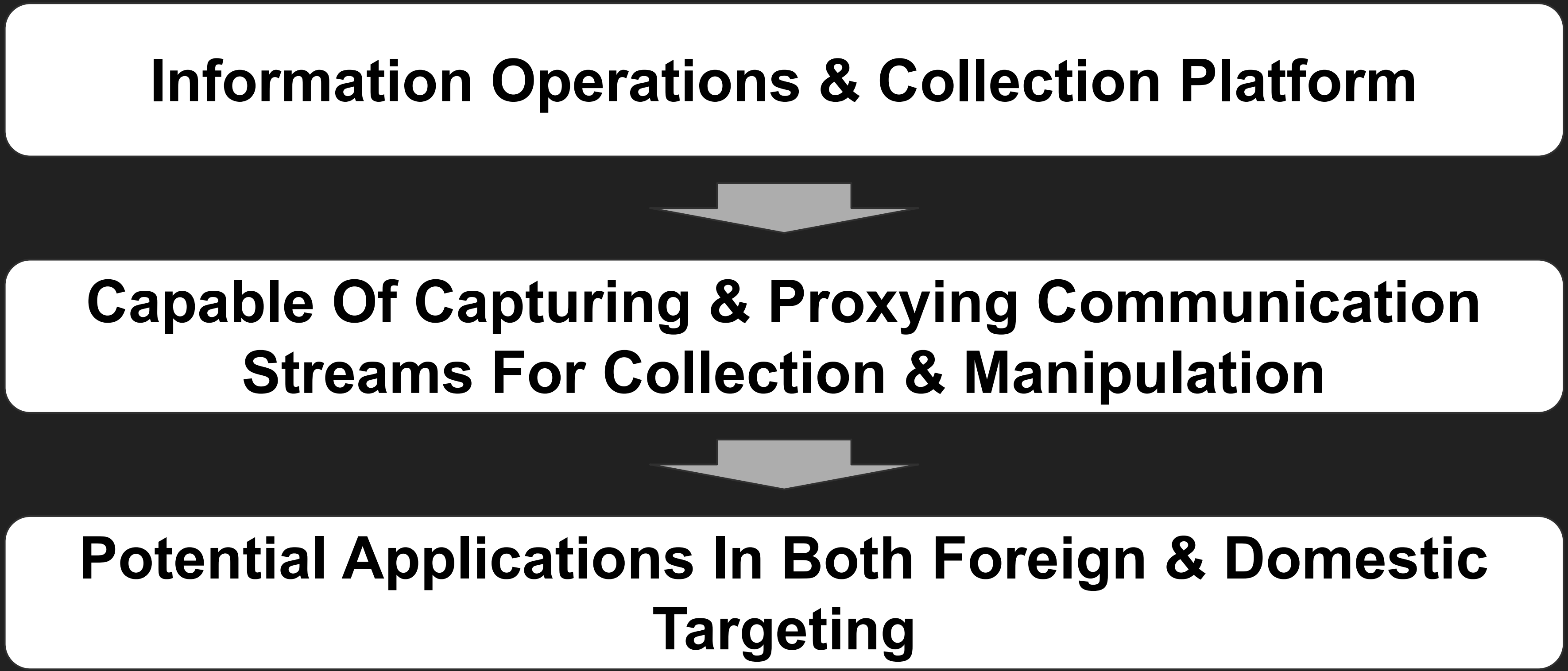
Information Operations & Collection Platform

Amesit

Information Operations & Collection Platform

Capable Of Capturing & Proxying Communication Streams For Collection & Manipulation

Amesit

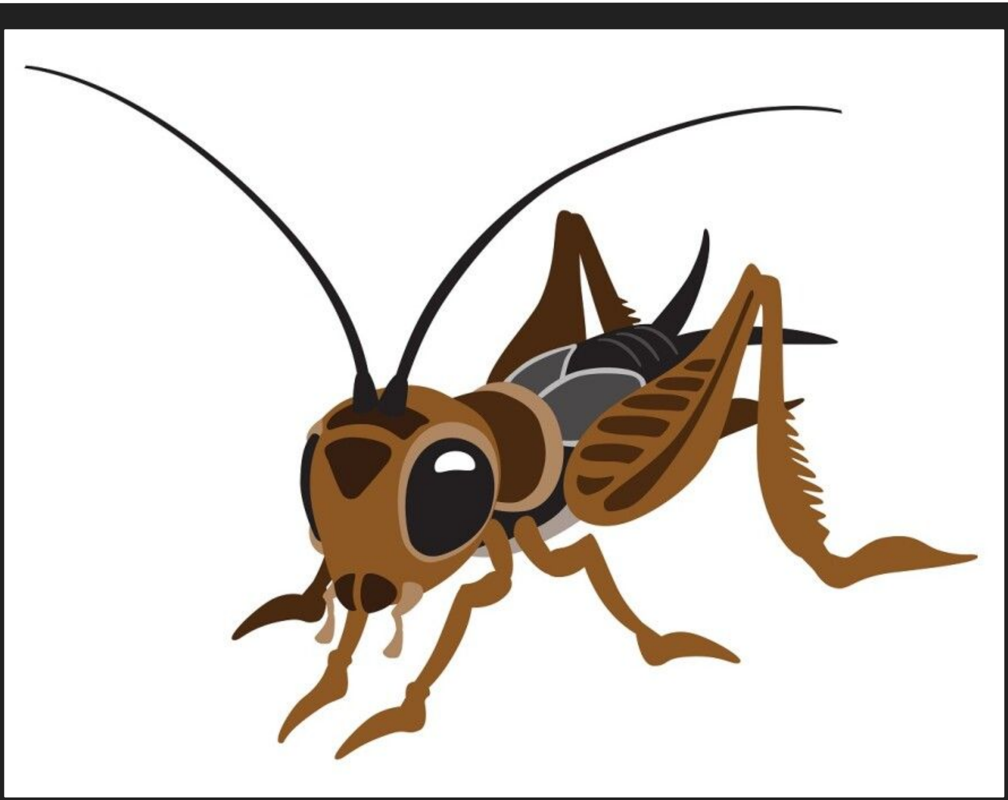


Information Operations & Collection Platform

Capable Of Capturing & Proxying Communication Streams For Collection & Manipulation

Potential Applications In Both Foreign & Domestic Targeting

Response To The Vulkan Leaks



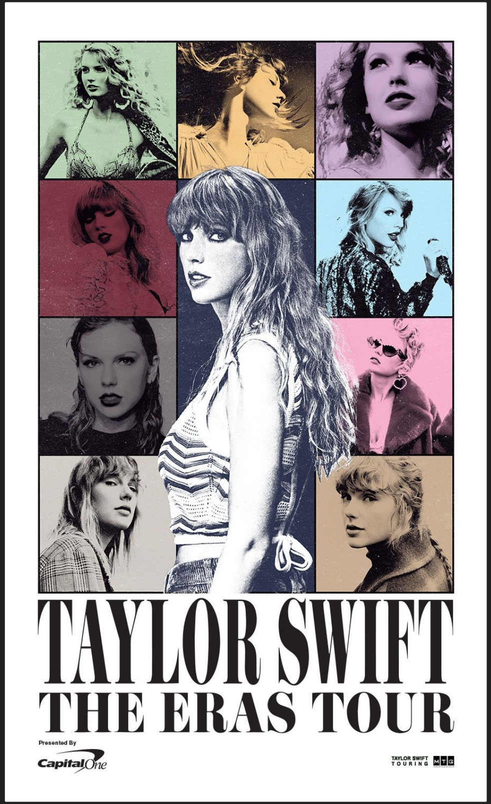
Response To The Vulkan Leaks

Response To The Vulkan Leaks

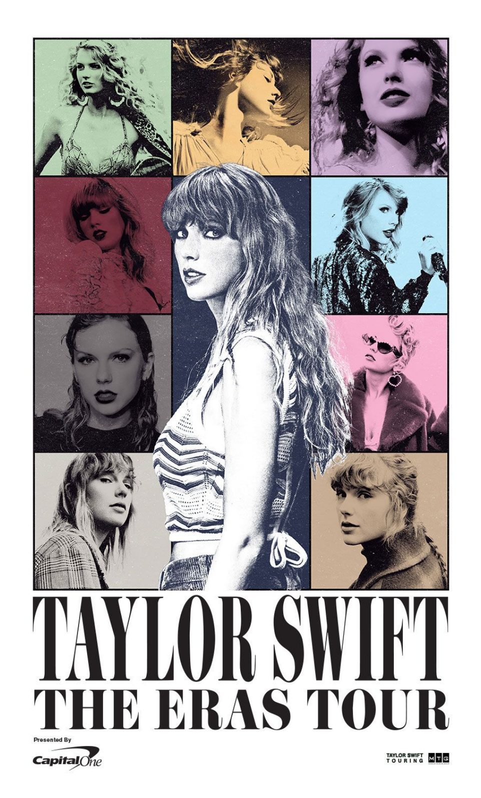
NEW YORK POST
DAILY NEWS
TRUMP INDICTED
1st ex-president to face criminal rap
Grand jury probed porn star payout
Set to surrender in NYC Tuesday
The New York Times
TRUMP INDICTED
THE FIRST EX-PRESIDENT TO FACE CRIMINAL CHA

Response To The Vulkan Leaks

NEW YORK POST
TRUMP INDICTED
DAILY NEWS
TRUMP INDICTED
1st ex-president to face criminal rap
Grand jury probed porn star payout
Set to surrender in NYC Tuesday
The New York Times
TRUMP INDICTED
THE FIRST EX-PRESIDENT TO FACE CRIMINAL CHA



Response To The Vulkan Leaks



Response To The Vulkan Leaks

Diving Into The Vulkan Leaks

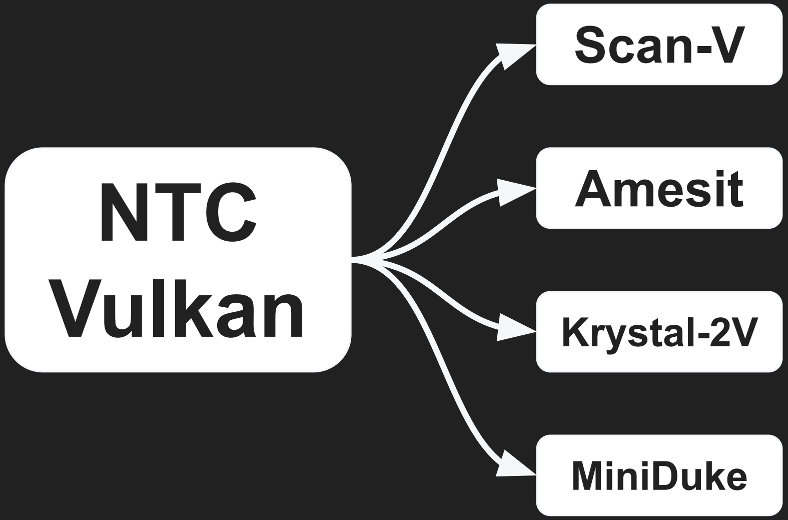
The Vulkan Leaks Represent A Significant Event In The History Of Cyber Operations - We Need To Review Just What’s Inside!

Vulkan & Russian Cyber Operations

Diving Into The Vulkan Leaks

NTC
Vulkan

Diving Into The Vulkan Leaks



NTC Vulkan

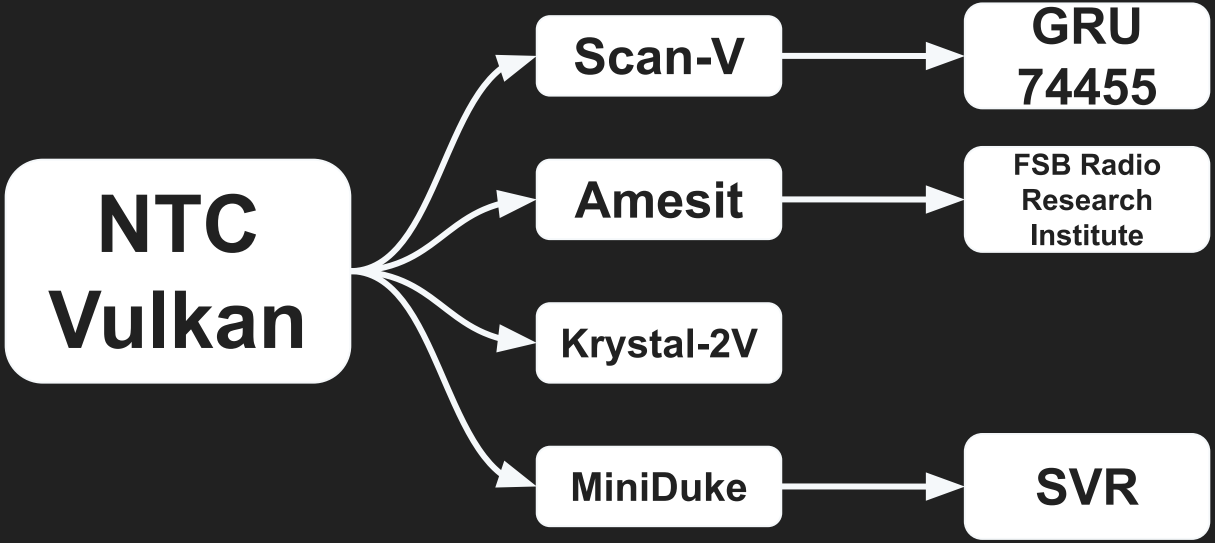
Scan-V

Amesit

Krystal-2V

MiniDuke

Diving Into The Vulkan Leaks



NTC Vulkan

Scan-V

Amesit

Krystal-2V

MiniDuke

GRU 74455

FSB Radio Research Institute

SVR

Vulkan & Russia’s “Cyber Hydra”

For Various Reasons, Research Institutes & External Entities Generally *Perform Dedicated Work For One Element Of Russia’s Cyber Forces…*

Vulkan & Russia’s “Cyber Hydra”

For Various Reasons, Research Institutes & External Entities Generally *Perform Dedicated Work For One Element Of Russia’s Cyber Forces…*

NTC Vulkan Worked With **EACH** ***Element Of Russian External Cyber Ops - GRU, FSB, & SVR - Not Completely Unique But Rare!***

RU Cyber & The Private Sector

RU Cyber & The Private Sector

TsNIIKhM & XENOTIME

RU Cyber & The Private Sector

TsNIIKhM & XENOTIME

SVA Institute & SVR

RU Cyber & The Private Sector

TsNIIKhM & XENOTIME

SVA Institute & SVR

ODT & FSB’s Fronton Botnet

RU Cyber & The Private Sector

TsNIIKhM & XENOTIME

SVA Institute & SVR

ODT & FSB’s Fronton Botnet

Kvant Institute & FSB

RU Cyber & The Private Sector

TsNIIKhM & XENOTIME

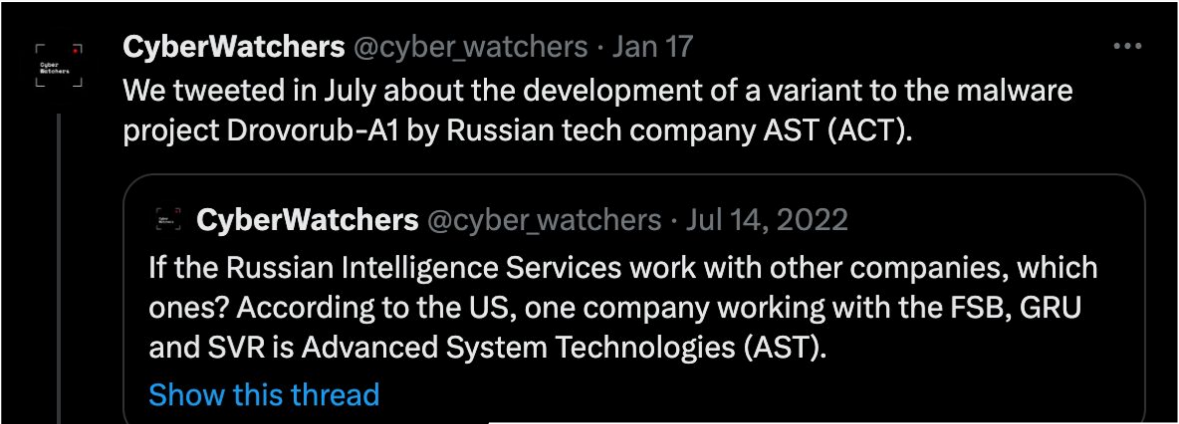
SVA Institute & SVR

ODT & FSB's Fronton Botnet

Kvant Institute & FSB

INCONTROLLER / PIPEDREAM?

RU Cyber & The Private Sector



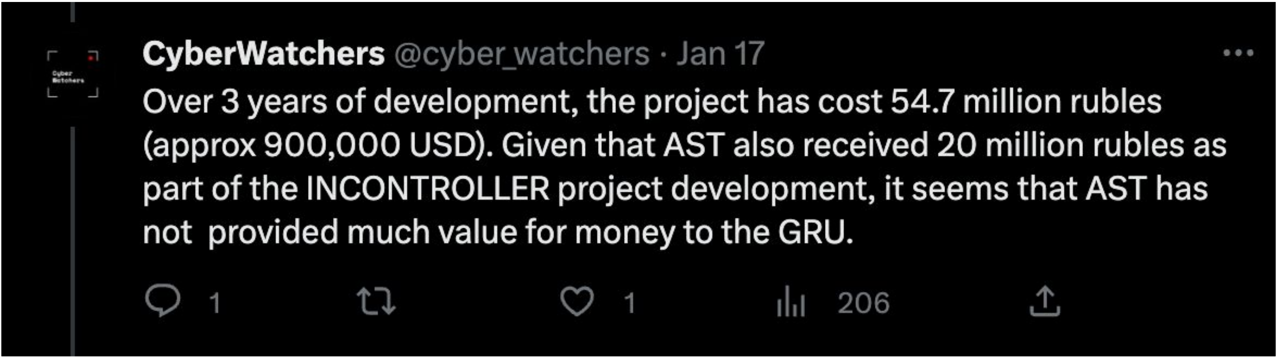
CyberWatchers @cyber_watchers · Jan 17

We tweeted in July about the development of a variant to the malware project Drovorub-A1 by Russian tech company AST (ACT).

> **CyberWatchers** @cyber_watchers · Jul 14, 2022
>
> If the Russian Intelligence Services work with other companies, which ones? According to the US, one company working with the FSB, GRU and SVR is Advanced System Technologies (AST).
>
> Show this thread

tute &
R

titute &
R



CyberWatchers @cyber_watchers · Jan 17

Over 3 years of development, the project has cost 54.7 million rubles (approx 900,000 USD). Given that AST also received 20 million rubles as part of the INCONTROLLER project development, it seems that AST has not provided much value for money to the GRU.

Privatization Of Cyber Development

NTC Vulkan Is Both An Example And A Pioneer Of Increasingly Outsourced Cyber Development & Engineering Work For State-Directed Operations!

Privatization Of Cyber Development

NTC Vulkan Is Both A [illegible] ample And A Pioneer Of In [illegible] utsourced Cyber Devel [illegible] eering Work For Stat [illegible] d Operations!

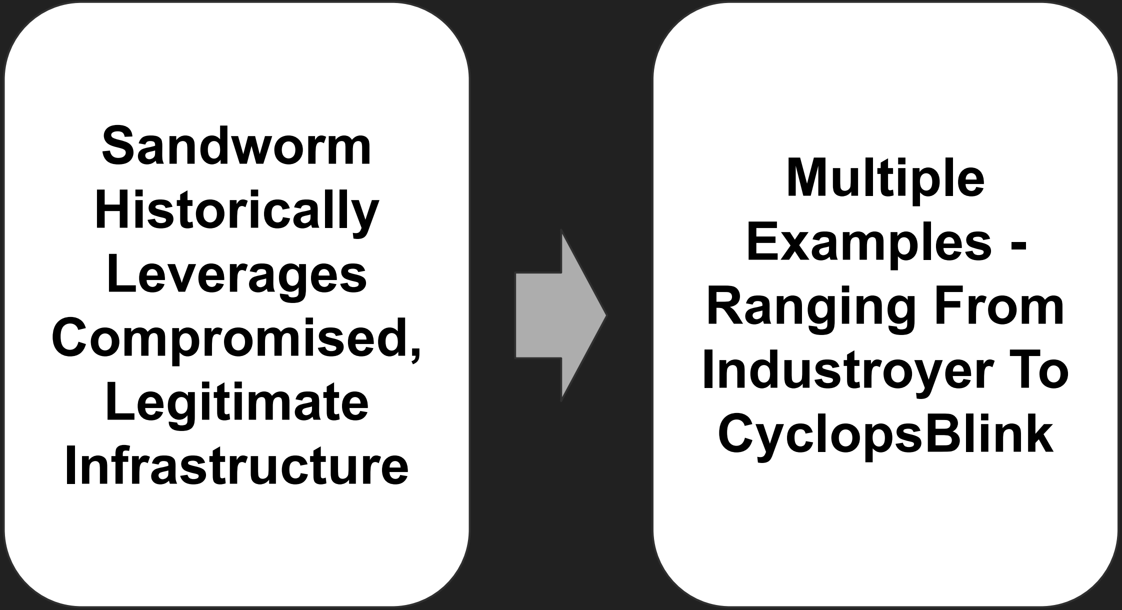
NOTE: This Is NOT Just Russia!

Scan-V & Sandworm

Scan-V & Sandworm

Sandworm Historically Leverages Compromised, Legitimate Infrastructure

Scan-V & Sandworm



Sandworm Historically Leverages Compromised, Legitimate Infrastructure

Multiple Examples - Ranging From Industroyer To CyclopsBlink

Scan-V & Sandworm

Sandworm Historically Leverages Compromised, Legitimate Infrastructure

Multiple Examples - Ranging From Industroyer To CyclopsBlink

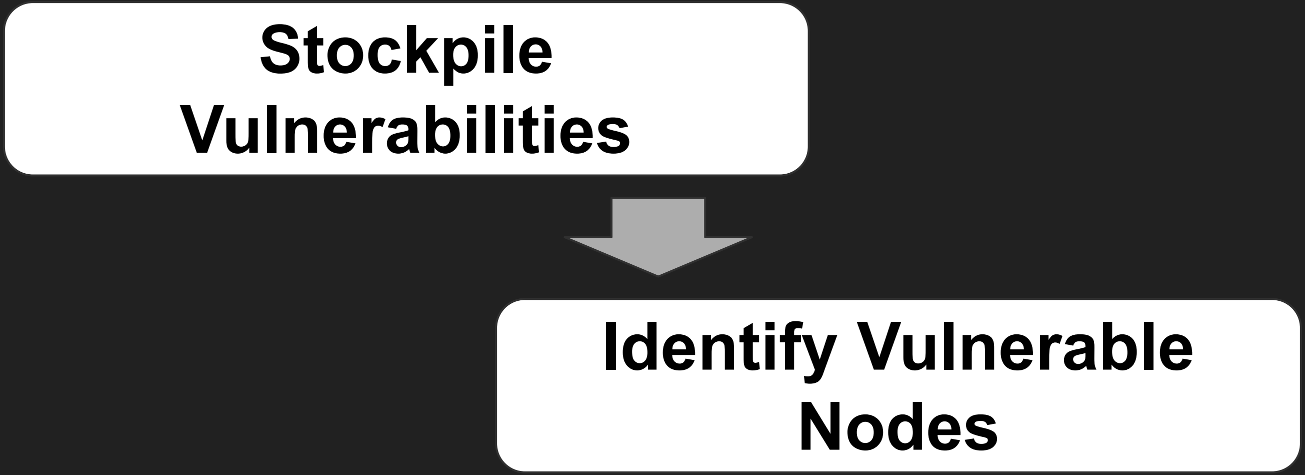
Building Out C2 Infrastructure Scales More Effectively With Automation!

Scan-V & Sandworm

Scan-V & Sandworm

Stockpile Vulnerabilities

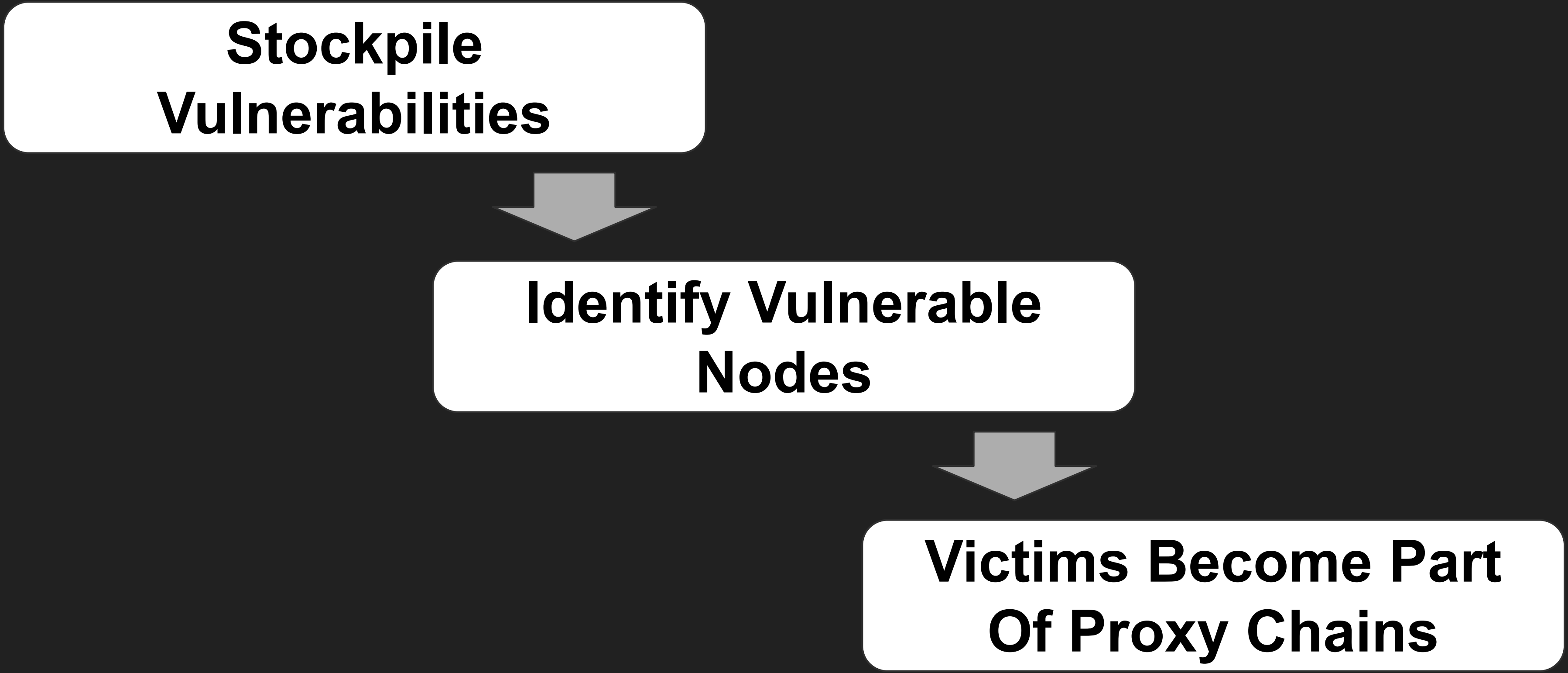
Scan-V & Sandworm



Stockpile Vulnerabilities

Identify Vulnerable Nodes

Scan-V & Sandworm



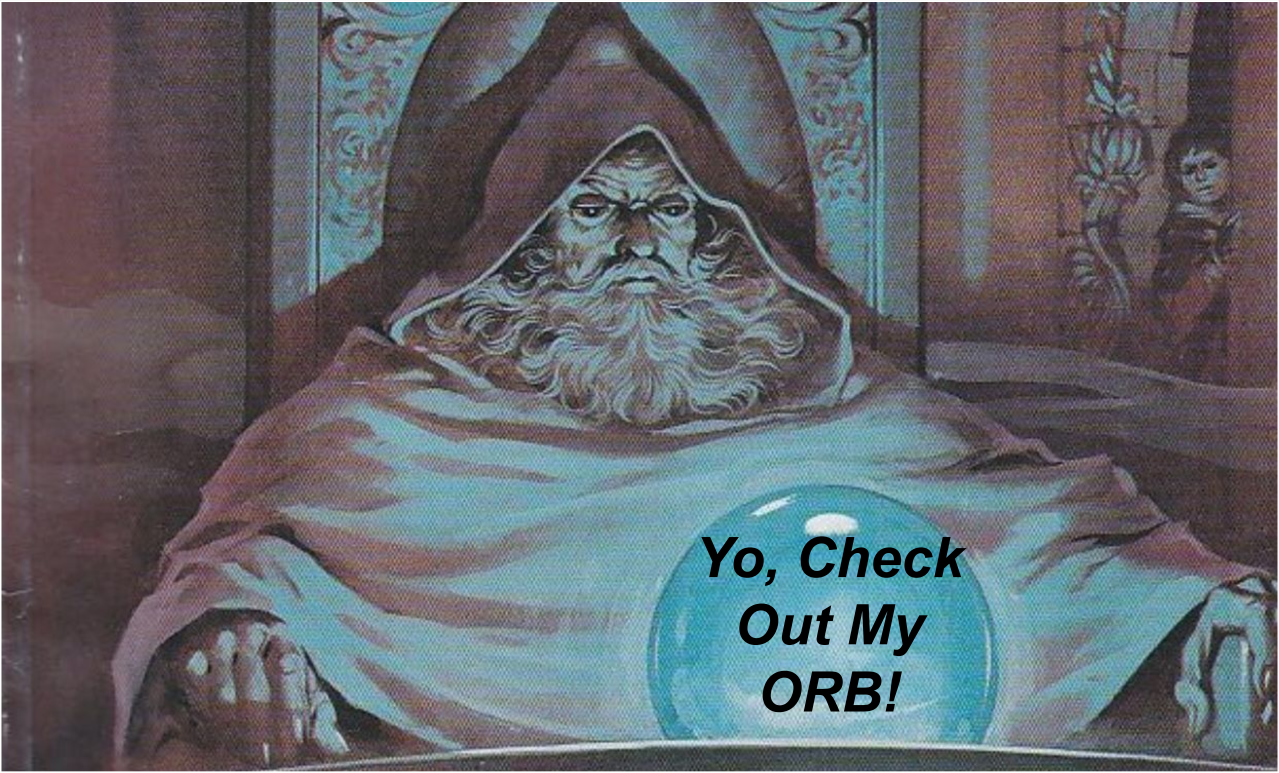
Stockpile Vulnerabilities

Identify Vulnerable Nodes

Victims Become Part Of Proxy Chains

Scan-V & Sandworm

Scan-V & Sandworm



The “So What” Behind Vulkan

The “So What” Behind Vulkan

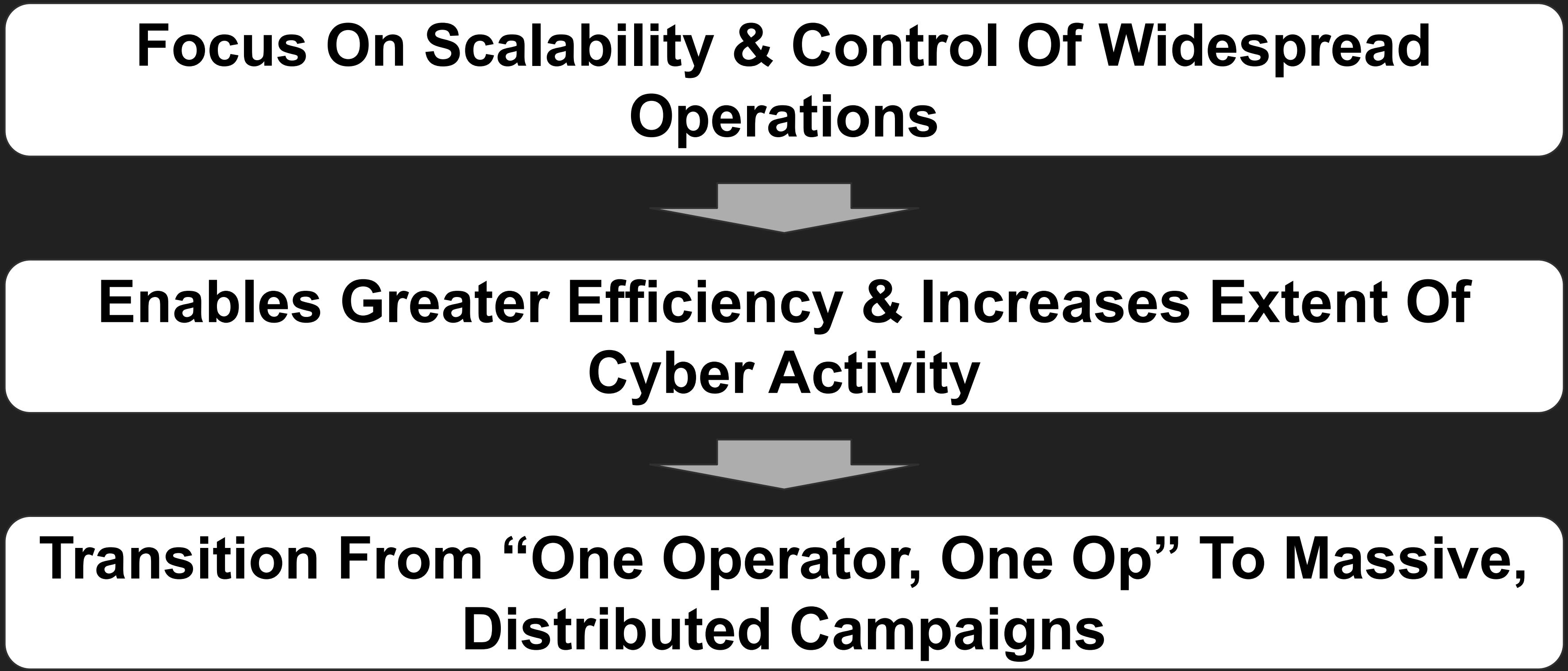
Focus On Scalability & Control Of Widespread Operations

The “So What” Behind Vulkan

Focus On Scalability & Control Of Widespread Operations

Enables Greater Efficiency & Increases Extent Of Cyber Activity

The “So What” Behind Vulkan



Focus On Scalability & Control Of Widespread Operations

Enables Greater Efficiency & Increases Extent Of Cyber Activity

Transition From “One Operator, One Op” To Massive, Distributed Campaigns

Vulkan In Cyber History

Is Vulkan Activity Unique?

Is Vulkan Activity Unique?

Scan-V - Similar Examples?

Scan-V - Similar Examples?

Russia!

Scan-V - Similar Examples?

Russia!

China!

Scan-V - Similar Examples?

Russia!

China!

USA?

Scan-V - Similar Examples?

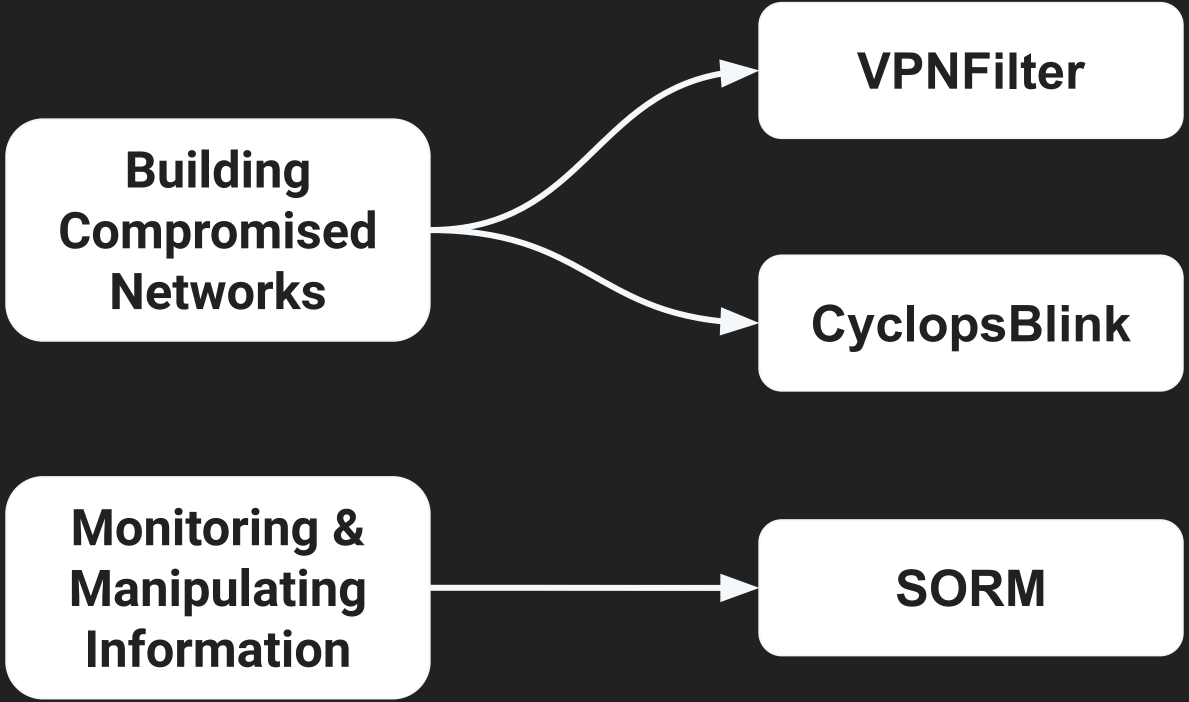
Russia & Cyber Manipulation

Russia & Cyber Manipulation

Building Compromised Networks

Monitoring & Manipulating Information

Russia & Cyber Manipulation



Building Compromised Networks

VPNFilter

CyclopsBlink

Monitoring & Manipulating Information

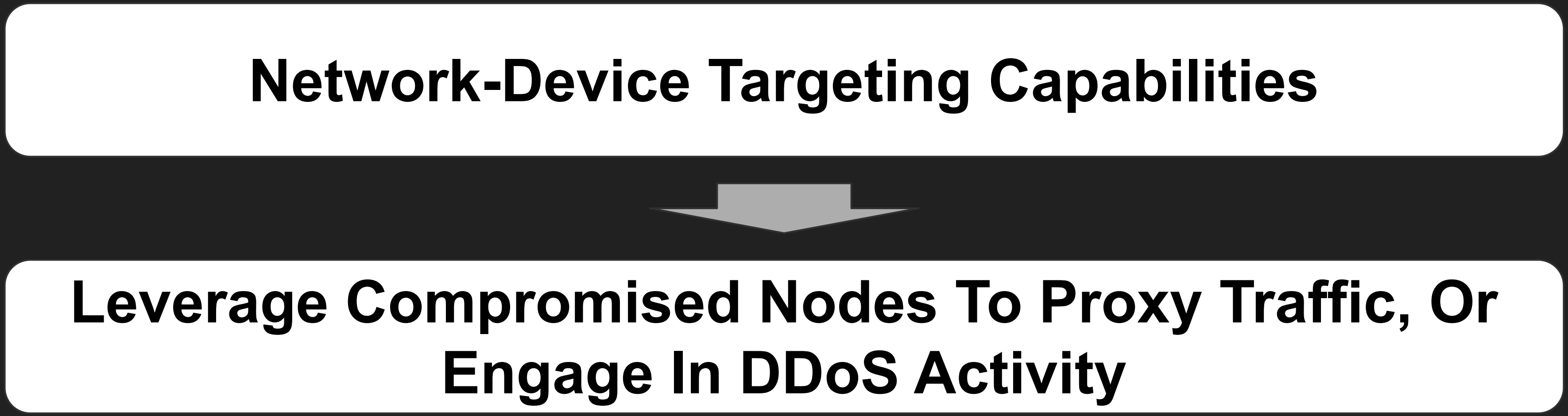
SORM

VPNFilter & CyclopsBlink

VPNFilter & CyclopsBlink

Network-Device Targeting Capabilities

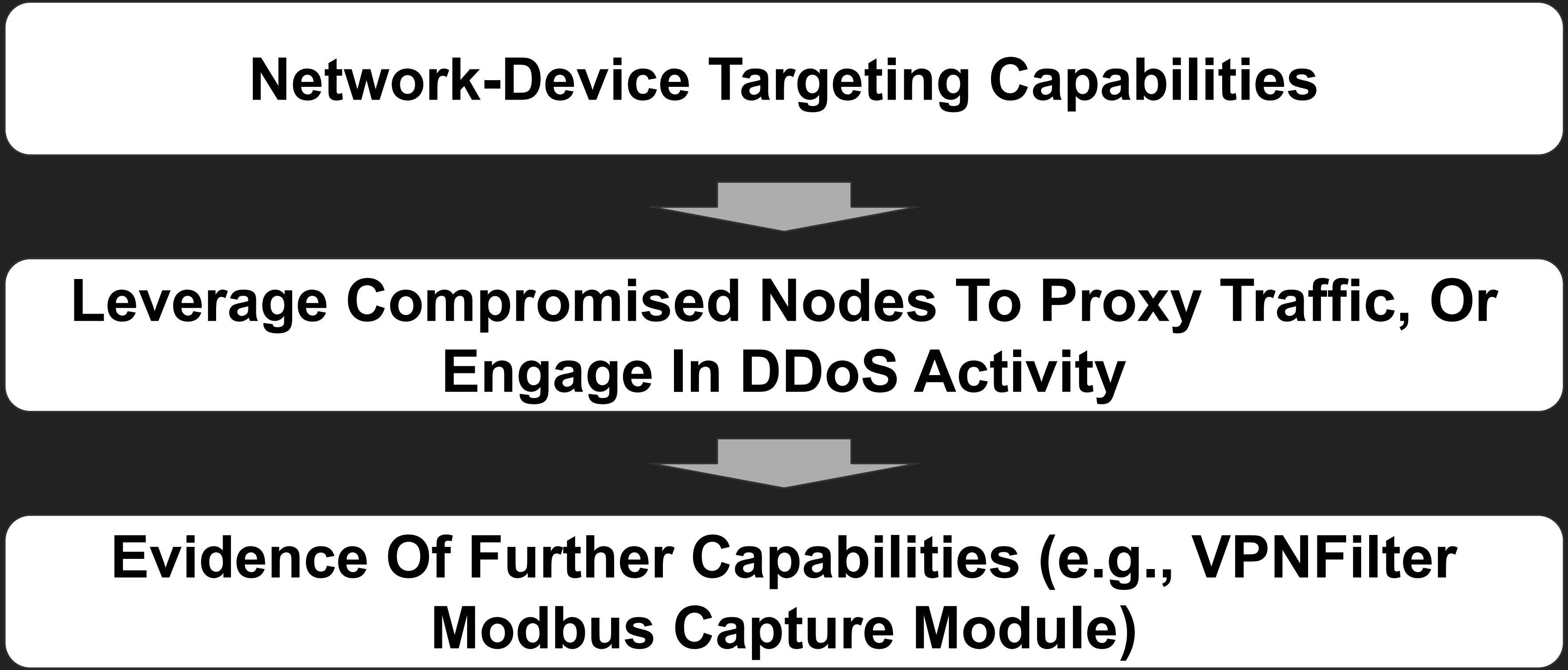
VPNFilter & CyclopsBlink



Network-Device Targeting Capabilities

Leverage Compromised Nodes To Proxy Traffic, Or Engage In DDoS Activity

VPNFilter & CyclopsBlink



Network-Device Targeting Capabilities

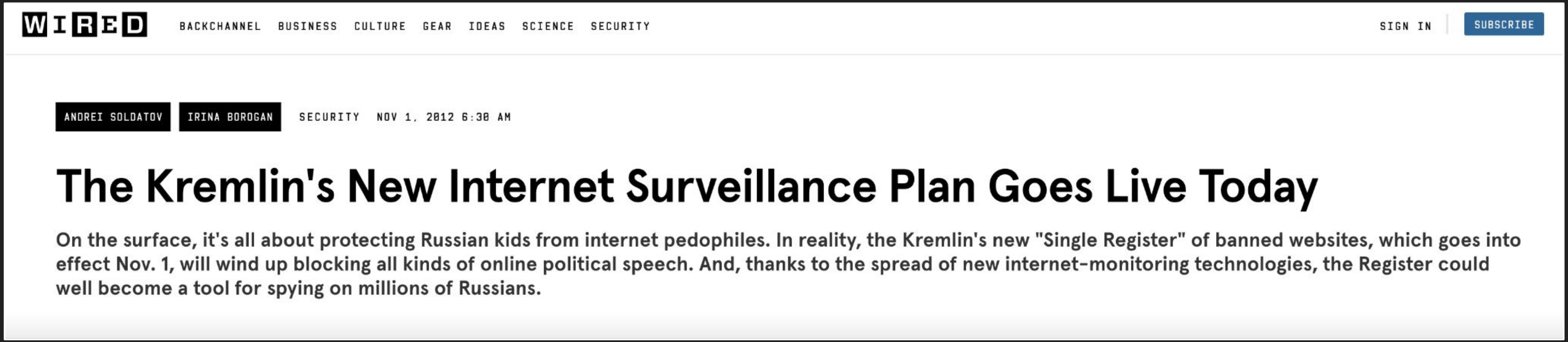
Leverage Compromised Nodes To Proxy Traffic, Or Engage In DDoS Activity

Evidence Of Further Capabilities (e.g., VPNFilter Modbus Capture Module)

VPNFilter & CyclopsBlink

Scan-V Represents A Mechanism To Automate, Control, & Manage A Network Of Collection Nodes & ORBs For Cyber Operations - Scalability & Efficiency!

SORM

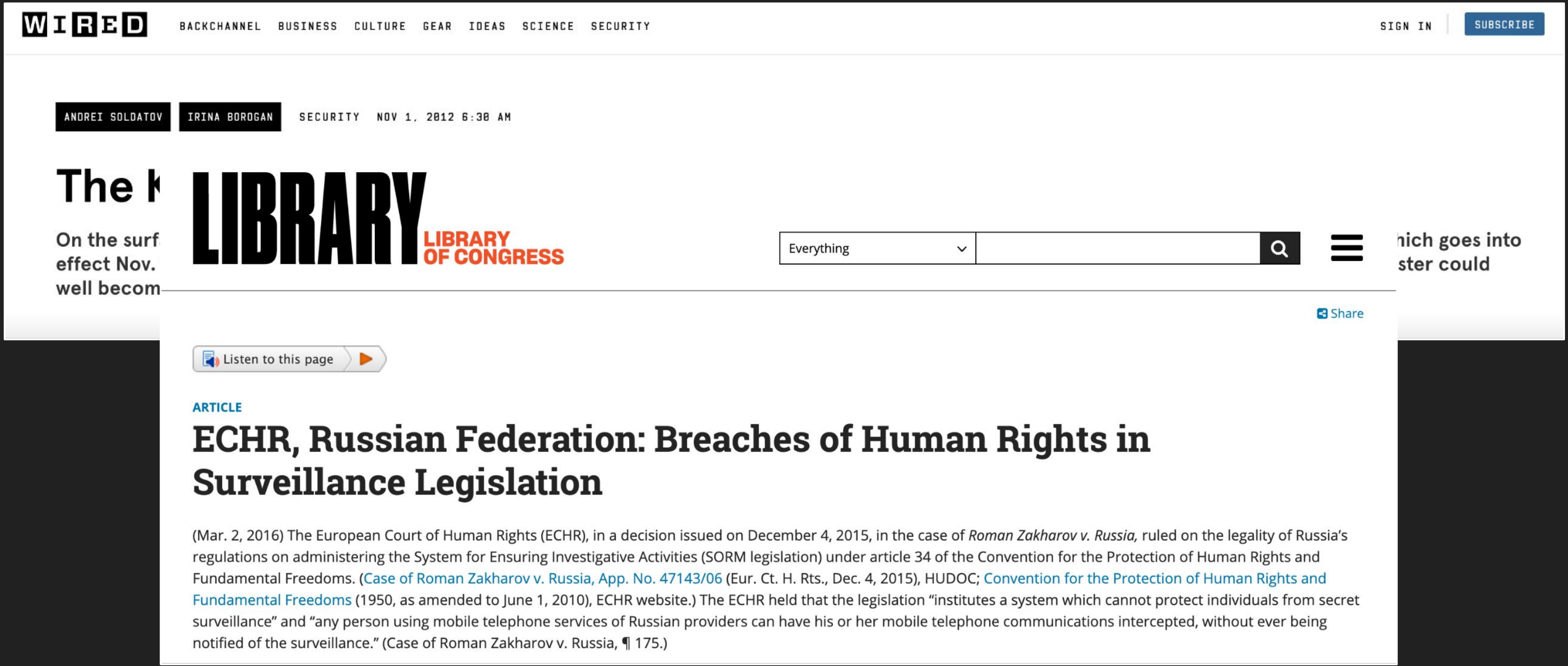


ANDREI SOLDATOV IRINA BOROGAN SECURITY NOV 1, 2012 6:30 AM

The Kremlin's New Internet Surveillance Plan Goes Live Today

On the surface, it's all about protecting Russian kids from internet pedophiles. In reality, the Kremlin's new "Single Register" of banned websites, which goes into effect Nov. 1, will wind up blocking all kinds of online political speech. And, thanks to the spread of new internet-monitoring technologies, the Register could well become a tool for spying on millions of Russians.

SORM



ANDREI SOLDATOV IRINA BOROGAN SECURITY NOV 1, 2012 6:30 AM

The k

On the surf … hich goes into
effect Nov. … ster could
well becom

ARTICLE

ECHR, Russian Federation: Breaches of Human Rights in Surveillance Legislation

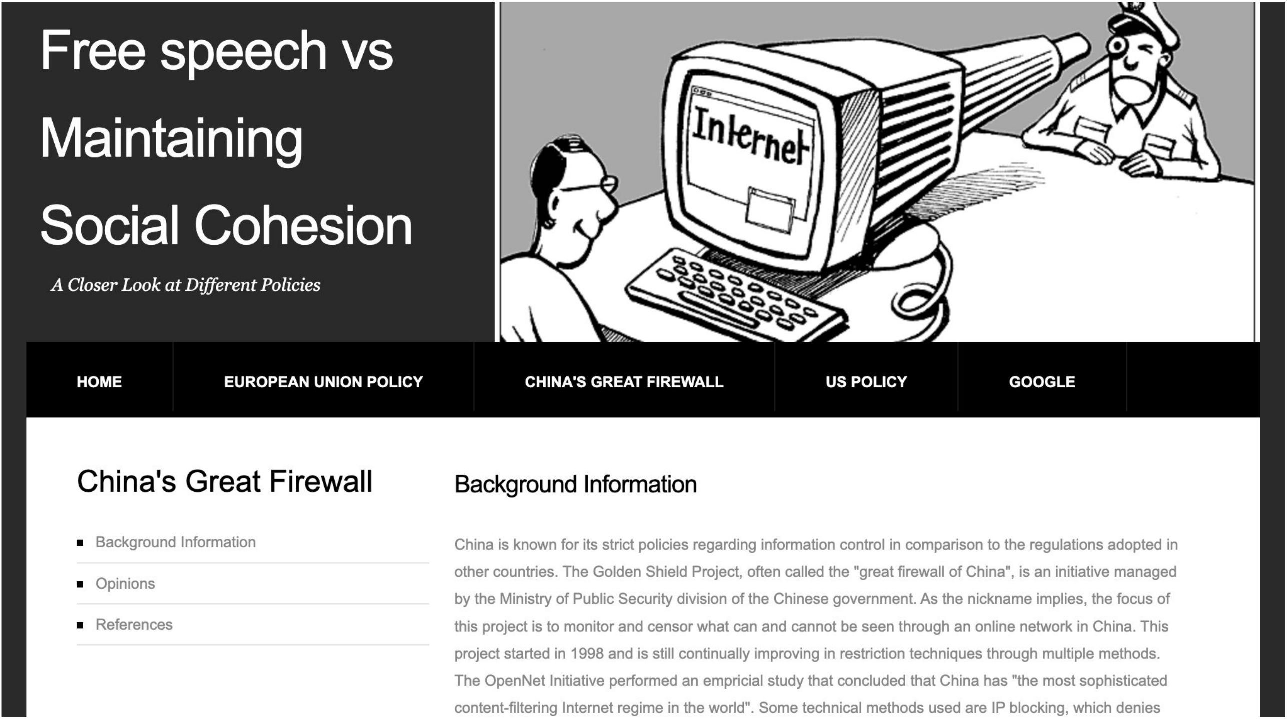
(Mar. 2, 2016) The European Court of Human Rights (ECHR), in a decision issued on December 4, 2015, in the case of *Roman Zakharov v. Russia,* ruled on the legality of Russia's regulations on administering the System for Ensuring Investigative Activities (SORM legislation) under article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms. (Case of Roman Zakharov v. Russia, App. No. 47143/06 (Eur. Ct. H. Rts., Dec. 4, 2015), HUDOC; Convention for the Protection of Human Rights and Fundamental Freedoms (1950, as amended to June 1, 2010), ECHR website.) The ECHR held that the legislation "institutes a system which cannot protect individuals from secret surveillance" and "any person using mobile telephone services of Russian providers can have his or her mobile telephone communications intercepted, without ever being notified of the surveillance." (Case of Roman Zakharov v. Russia, ¶ 175.)

SORM To Amesit

Amesit Enables A Mobile, Flexible Deployment Of SORM-Like Capabilities, Including For INFORMATION & INFLUENCE OPERATION PURPOSES. Can Also Be "Forward Deployed."

What About PRC?

What About PRC?



Free speech vs Maintaining Social Cohesion

A Closer Look at Different Policies

HOME | EUROPEAN UNION POLICY | CHINA'S GREAT FIREWALL | US POLICY | GOOGLE

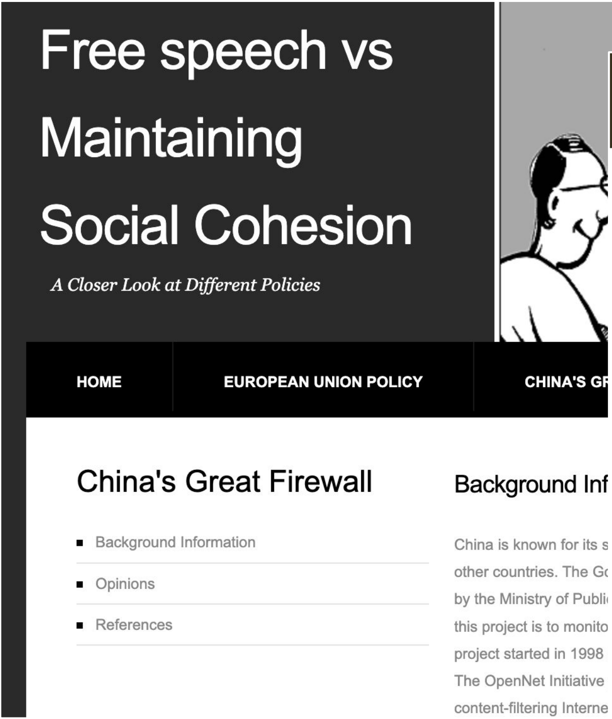
China's Great Firewall

- Background Information
- Opinions
- References

Background Information

China is known for its strict policies regarding information control in comparison to the regulations adopted in other countries. The Golden Shield Project, often called the "great firewall of China", is an initiative managed by the Ministry of Public Security division of the Chinese government. As the nickname implies, the focus of this project is to monitor and censor what can and cannot be seen through an online network in China. This project started in 1998 and is still continually improving in restriction techniques through multiple methods. The OpenNet Initiative performed an empricial study that concluded that China has "the most sophisticated content-filtering Internet regime in the world". Some technical methods used are IP blocking, which denies

What About PRC?



Free speech vs Maintaining Social Cohesion

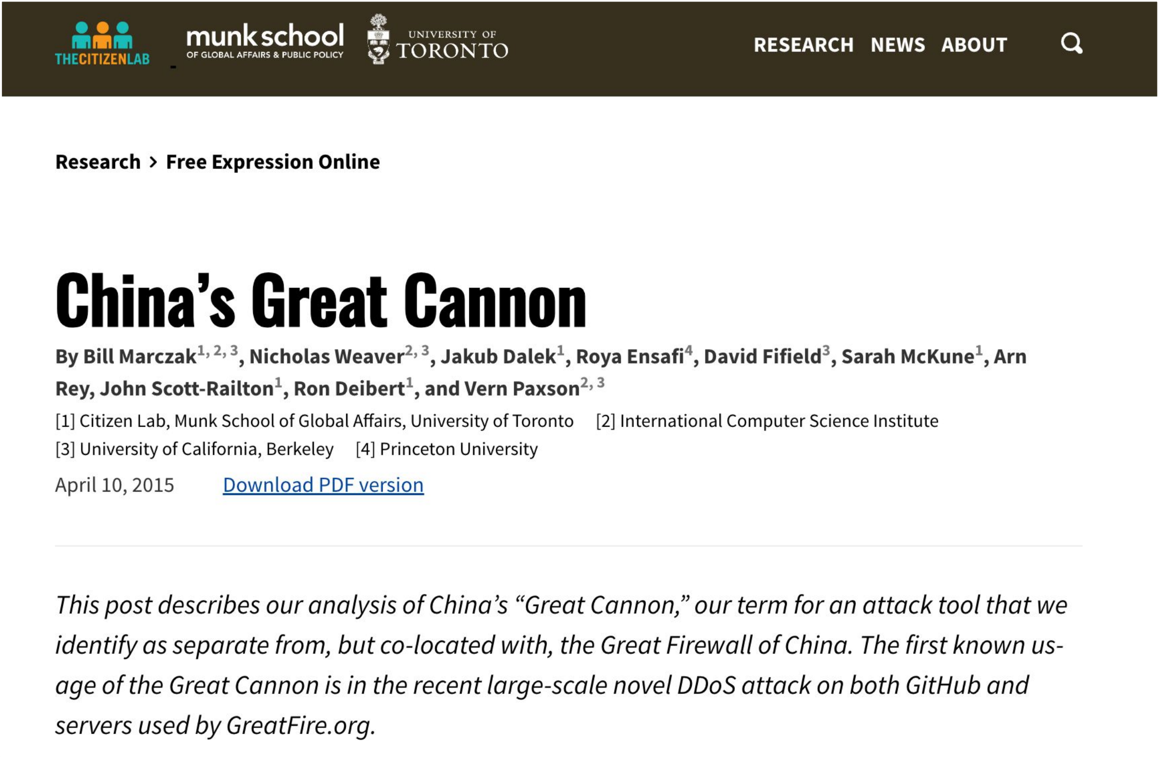
A Closer Look at Different Policies

China's Great Firewall

- Background Information
- Opinions
- References

Background Inf

China is known for its s
other countries. The Go
by the Ministry of Publi
this project is to monito
project started in 1998
The OpenNet Initiative
content-filtering Interne



Research › Free Expression Online

China's Great Cannon

By Bill Marczak[1, 2, 3], Nicholas Weaver[2, 3], Jakub Dalek[1], Roya Ensafi[4], David Fifield[3], Sarah McKune[1], Arn Rey, John Scott-Railton[1], Ron Deibert[1], and Vern Paxson[2, 3]

[1] Citizen Lab, Munk School of Global Affairs, University of Toronto [2] International Computer Science Institute
[3] University of California, Berkeley [4] Princeton University

April 10, 2015 Download PDF version

This post describes our analysis of China's "Great Cannon," our term for an attack tool that we identify as separate from, but co-located with, the Great Firewall of China. The first known usage of the Great Cannon is in the recent large-scale novel DDoS attack on both GitHub and servers used by GreatFire.org.

What About PRC?

Free speech vs

Maintaining

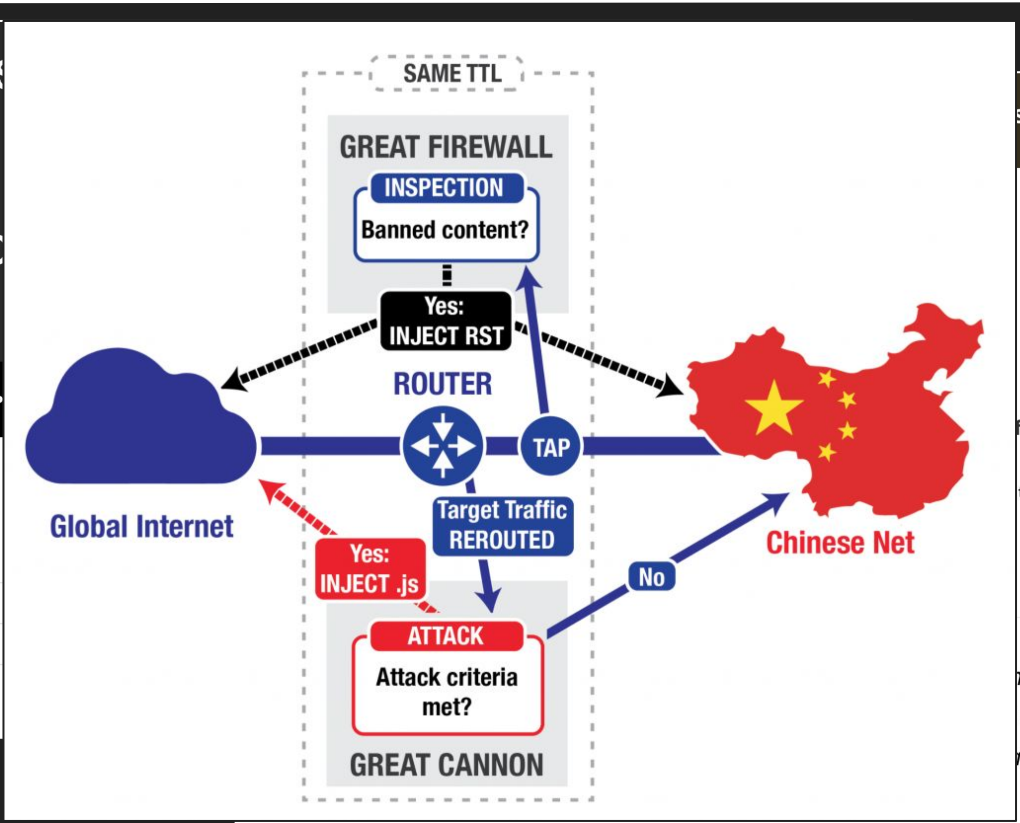
Social Cohesio

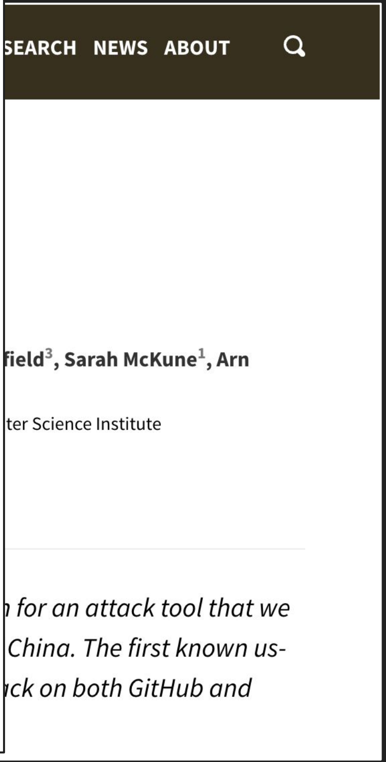
A Closer Look at Different Policies

HOME EUROPEAN UNION P

China's Great Firewall

- Background Information
- Opinions
- References





SEARCH NEWS ABOUT

field[3], Sarah McKune[1], Arn

ter Science Institute

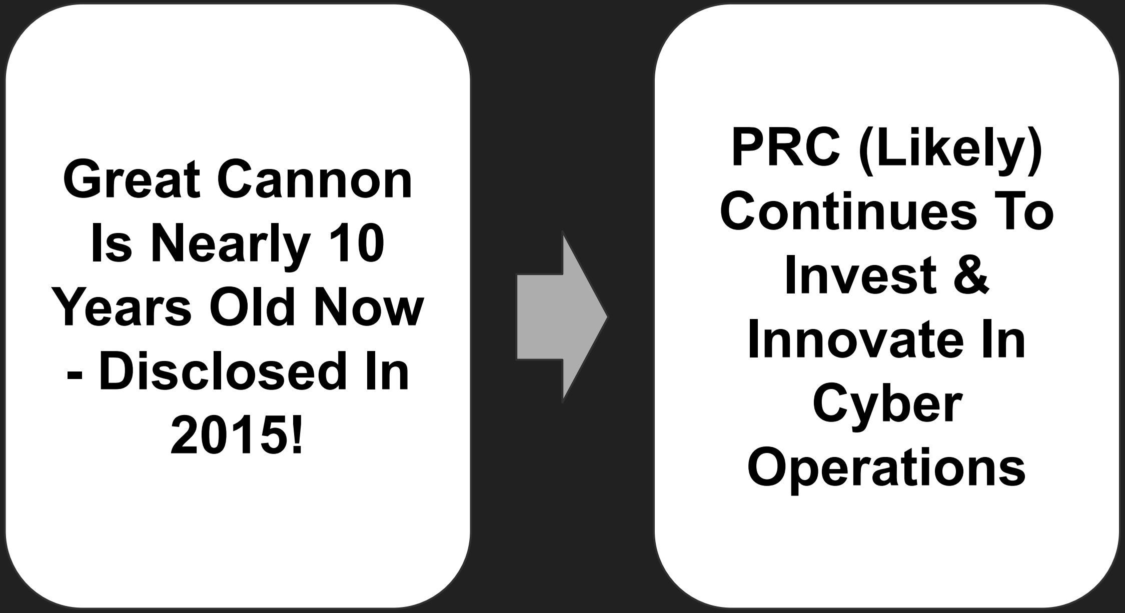
for an attack tool that we
China. The first known us-
ack on both GitHub and

PRC CNO & IO Operations

PRC CNO & IO Operations

Great Cannon Is Nearly 10 Years Old Now - Disclosed In 2015!

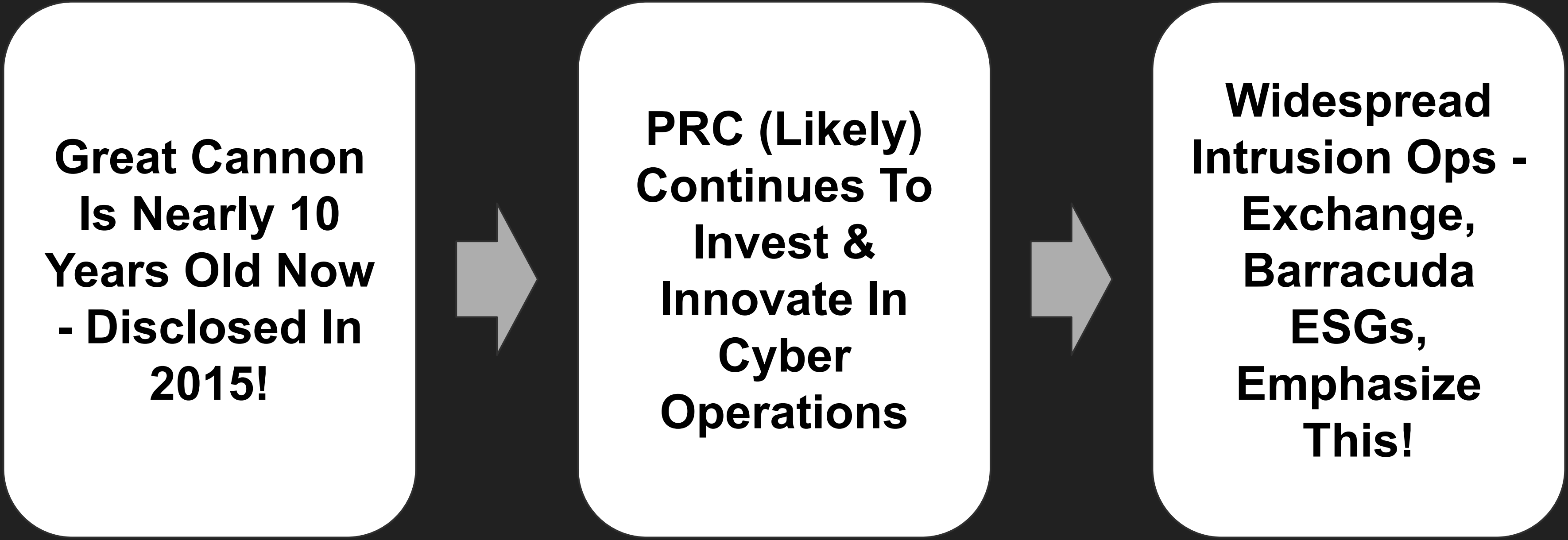
PRC CNO & IO Operations



Great Cannon Is Nearly 10 Years Old Now - Disclosed In 2015!

PRC (Likely) Continues To Invest & Innovate In Cyber Operations

PRC CNO & IO Operations



Great Cannon Is Nearly 10 Years Old Now - Disclosed In 2015!

PRC (Likely) Continues To Invest & Innovate In Cyber Operations

Widespread Intrusion Ops - Exchange, Barracuda ESGs, Emphasize This!

PRC CNO & IO Operations

Great Firewall & Great Cannon Functionality Give Glimpses Of Similar Ambitions & Programs - Main Question Is Scalability & Management Of These Capabilities & Widespread Intrusion Campaigns

The United States & FVEY

Hey - Remember The Snowden Leaks?

The United States & FVEY

NOTE THAT THE FOLLOWING SLIDES
ARE BASED ON PUBLIC COMMENTARY
AND POSTING HERE NEITHER
CONFIRMS NOR DENIES THE ACCURACY
OR VERACITY OF THESE ITEMS!

NSA Leaks & Implications

NSA Leaks & Implications

Popular Conception

NSA Leaks & Implications

Popular Conception

- Emphasis On Privacy Violations & Other Elements Detrimental To Open Democracies
- Clearly Important - But Hardly The Limit Of What Was Disclosed

NSA Leaks & Implications

Popular Conception

- Emphasis On Privacy Violations & Other Elements Detrimental To Open Democracies
- Clearly Important - But Hardly The Limit Of What Was Disclosed

Additional Details

NSA Leaks & Implications

Popular Conception

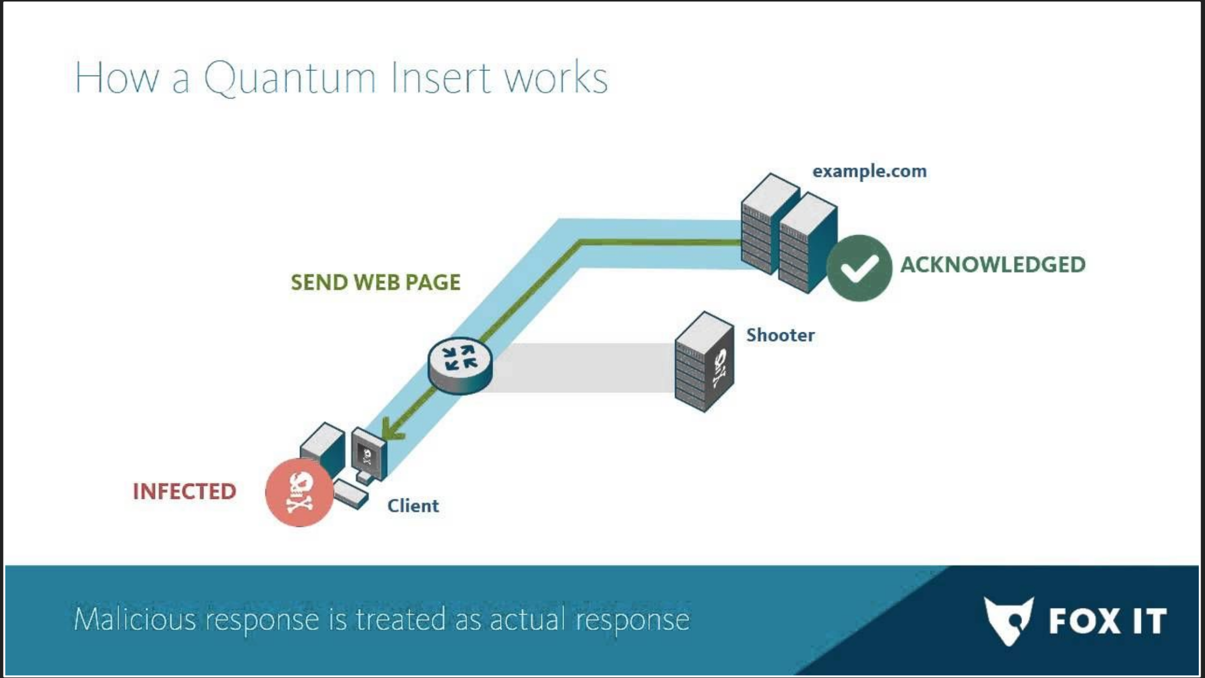
- Emphasis On Privacy Violations & Other Elements Detrimental To Open Democracies
- Clearly Important - But Hardly The Limit Of What Was Disclosed

Additional Details

- Snowden (And Potentially Others) Disclosed SIGNIFICANT Information On CNO Capabilities & Tradecraft Beyond Privacy & Legality Issues!
- Less-Heralded But Arguably More Significant Were Widespread, Automated Exploitation & Control Frameworks

A Quantum Of Exploitation

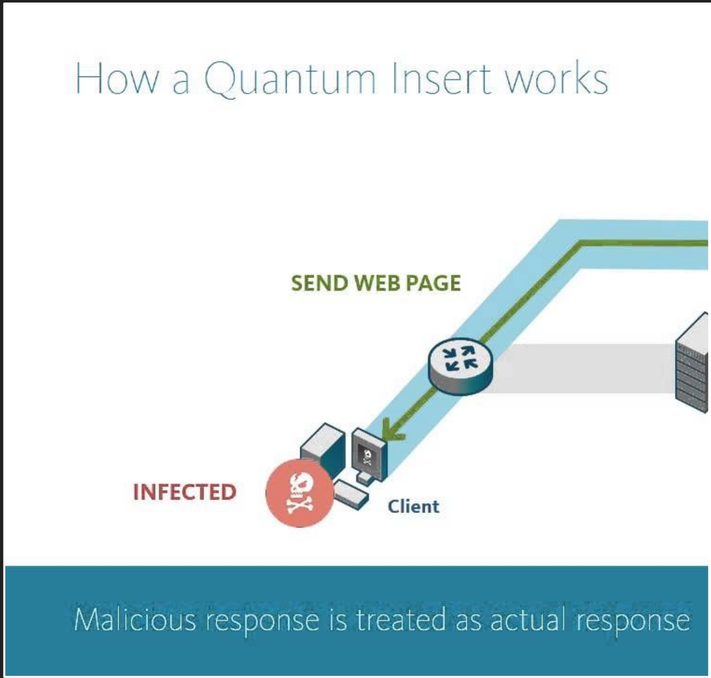
A Quantum Of Exploitation



How a Quantum Insert works

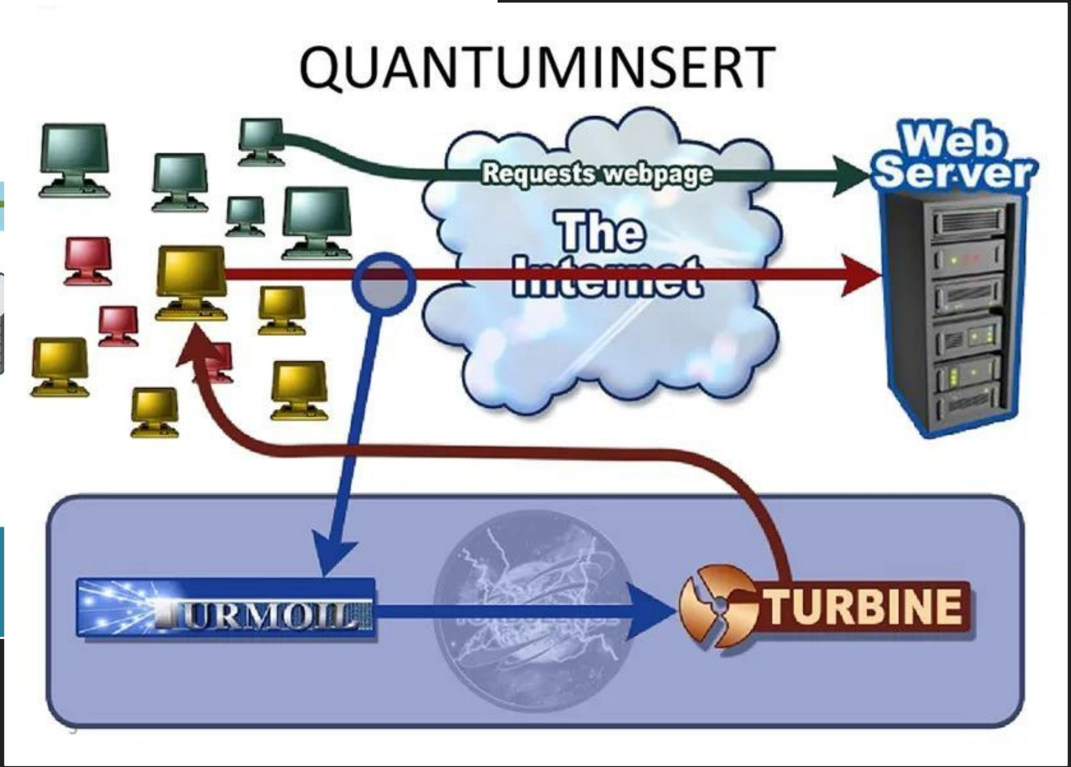
Malicious response is treated as actual response

A Quantum Of Exploitation



How a Quantum Insert works

Malicious response is treated as actual response



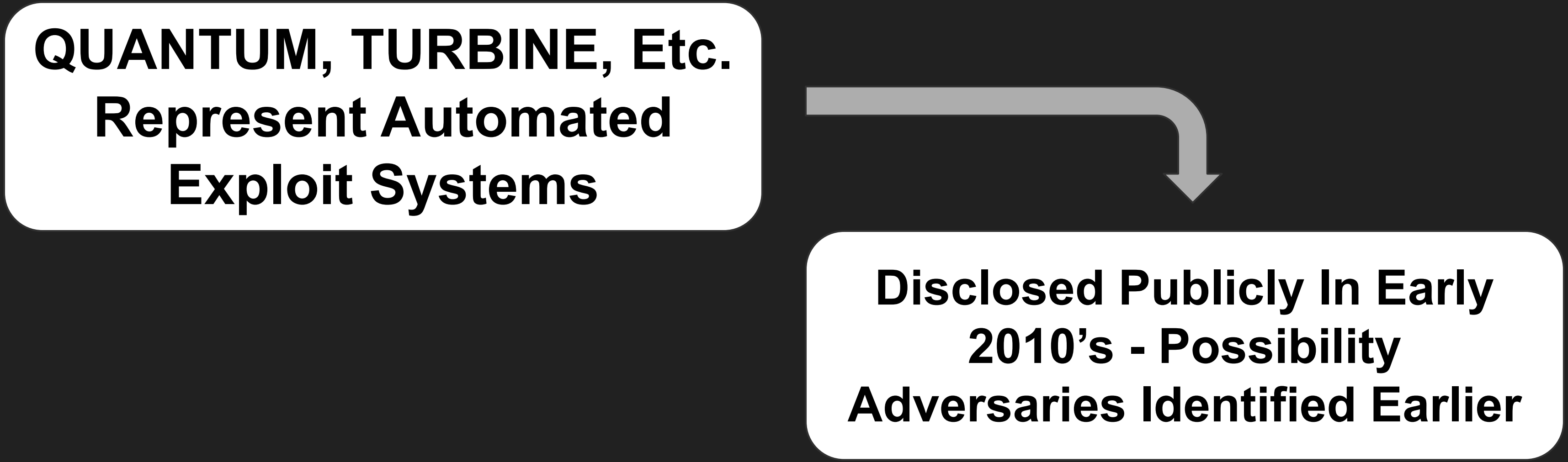
QUANTUMINSERT

Automated Exploitation At Scale

Automated Exploitation At Scale

QUANTUM, TURBINE, Etc. Represent Automated Exploit Systems

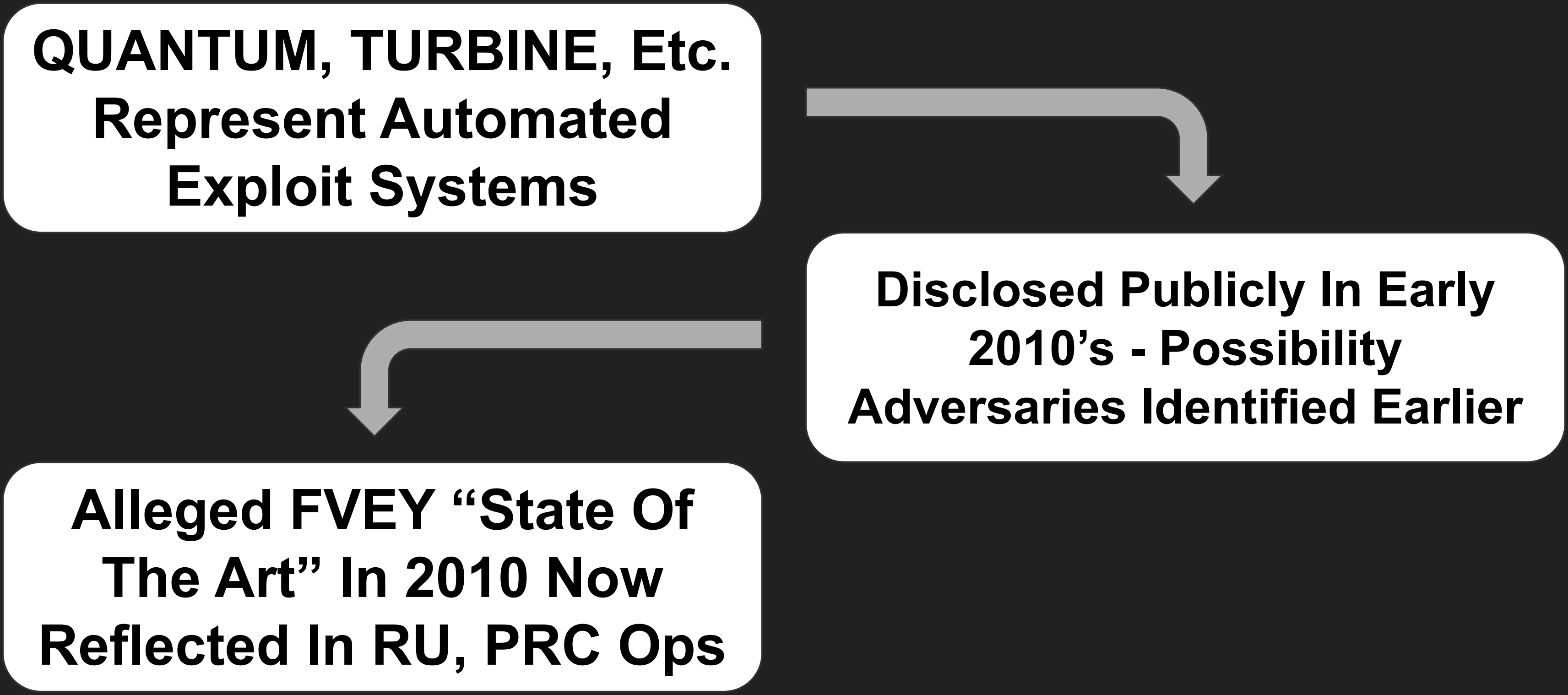
Automated Exploitation At Scale



QUANTUM, TURBINE, Etc. Represent Automated Exploit Systems

Disclosed Publicly In Early 2010’s - Possibility Adversaries Identified Earlier

Automated Exploitation At Scale



QUANTUM, TURBINE, Etc. Represent Automated Exploit Systems

Disclosed Publicly In Early 2010’s - Possibility Adversaries Identified Earlier

Alleged FVEY “State Of The Art” In 2010 Now Reflected In RU, PRC Ops

Snowden, Vulkan, & Beyond

IF TRUE - Snowden Leaks Were Arguably A DISASTER For US, Related CNO & SIGINT Capabilities By Disclosing Methodology…

Snowden, Vulkan, & Beyond

IF TRUE - Snowden Leaks Were Arguably A DISASTER For US, Related CNO & SIGINT Capabilities By Disclosing Methodology…

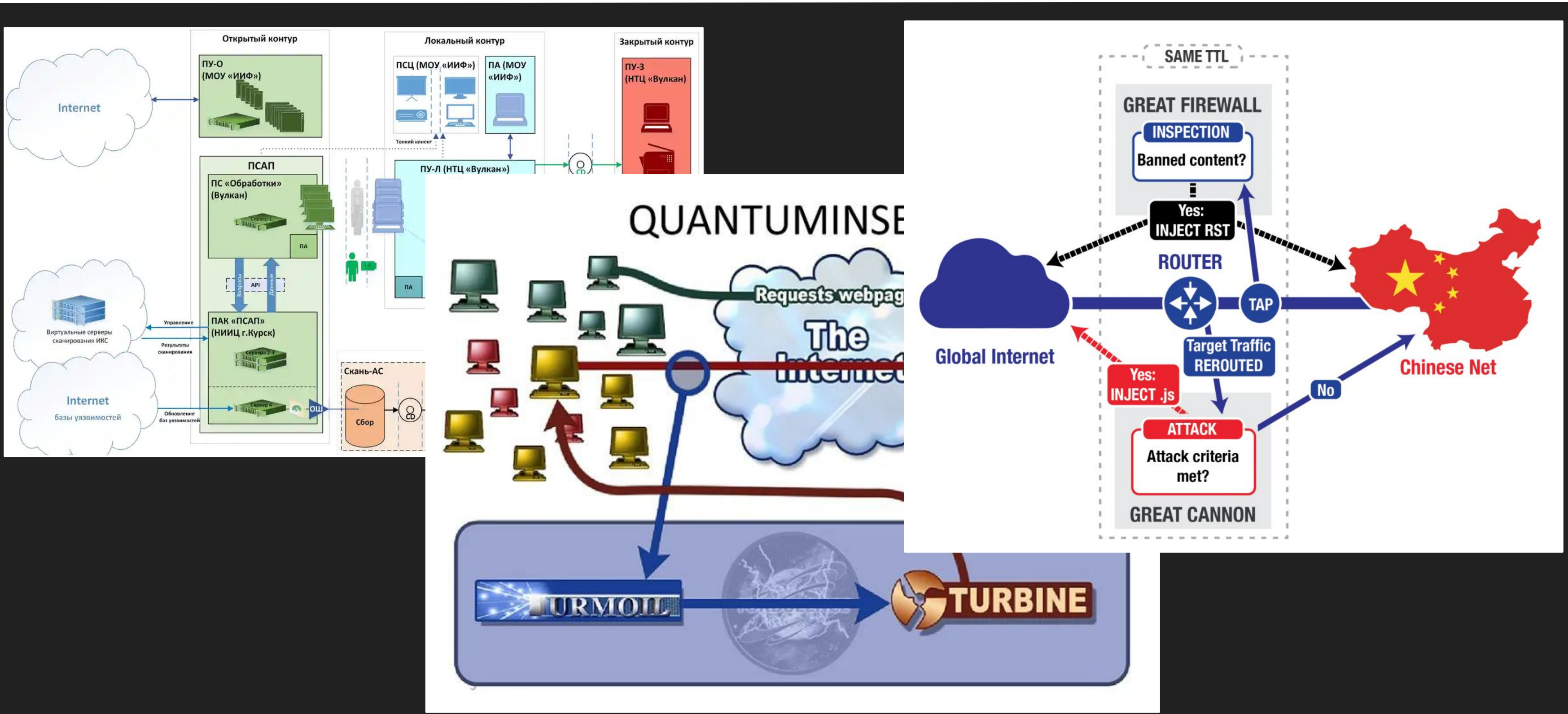
…It Also Appears That Multiple Parties Were Taking Notes On How To Build Similar (Or More Ambitious) Programs Based On Disclosures!

The Future Of Offensive Cyber

Popular Conception Of CNO

Realistic Depiction Of CNO

Future Applications Of CNO



The Road To Scalable Cyber

The Road To Scalable Cyber

Personnel

Cyber Talent Is Expensive - Codifying Capabilities In Technology & Programs Is Key To Expansive & Efficient Action!

The Road To Scalable Cyber

Personnel

Cyber Talent Is Expensive - Codifying Capabilities In Technology & Programs Is Key To Expansive & Efficient Action!

Targeting

Global Ambitions Require Global Actions. Assumptions On Targeting & Focus Go Out The Window - Especially When Targets Can Be “Means To An End!”

The Road To Scalable Cyber

Personnel

Cyber Talent Is Expensive - Codifying Capabilities In Technology & Programs Is Key To Expansive & Efficient Action!

Targeting

Global Ambitions Require Global Actions. Assumptions On Targeting & Focus Go Out The Window - Especially When Targets Can Be "Means To An End!"

Operational Security

Top-Tier Threat Actors Know How Defenders & CTI Analysts Operate - They Will Work To Evade Known Analytical Tradecraft & Minimize Touchpoints Wherever Possible!

NTC Vulkan & CNO

Vulkan Capabilities Are LAGGING Indicators - This Activity Has Already Taken Place!

NTC Vulkan & CNO

Vulkan Capabilities Are LAGGING Indicators - This Activity Has Already Taken Place!

We Need To Anticipate Greater Degrees Of Automation, Queueing, & Reactive Targeting!

What Should We Expect?

What Should We Expect?

Greater Automation & Improved Scalability

What Should We Expect?

Greater Automation & Improved Scalability

Leverage "Neutral Web" For Offensive Action

What Should We Expect?

Greater Automation & Improved Scalability

Leverage "Neutral Web" For Offensive Action

Reduced Reliance On "Rockstars" - Commoditization

What Should We Expect?

Greater Automation & Improved Scalability

Leverage “Neutral Web” For Offensive Action

Reduced Reliance On “Rockstars” - Commoditization

Actual, Meaningful Applications Of ML/AI

Conclusions

Where Are We Now?

Where Are We Now?

But…

Capability Inspiration & Proliferation

Capability Inspiration & Proliferation

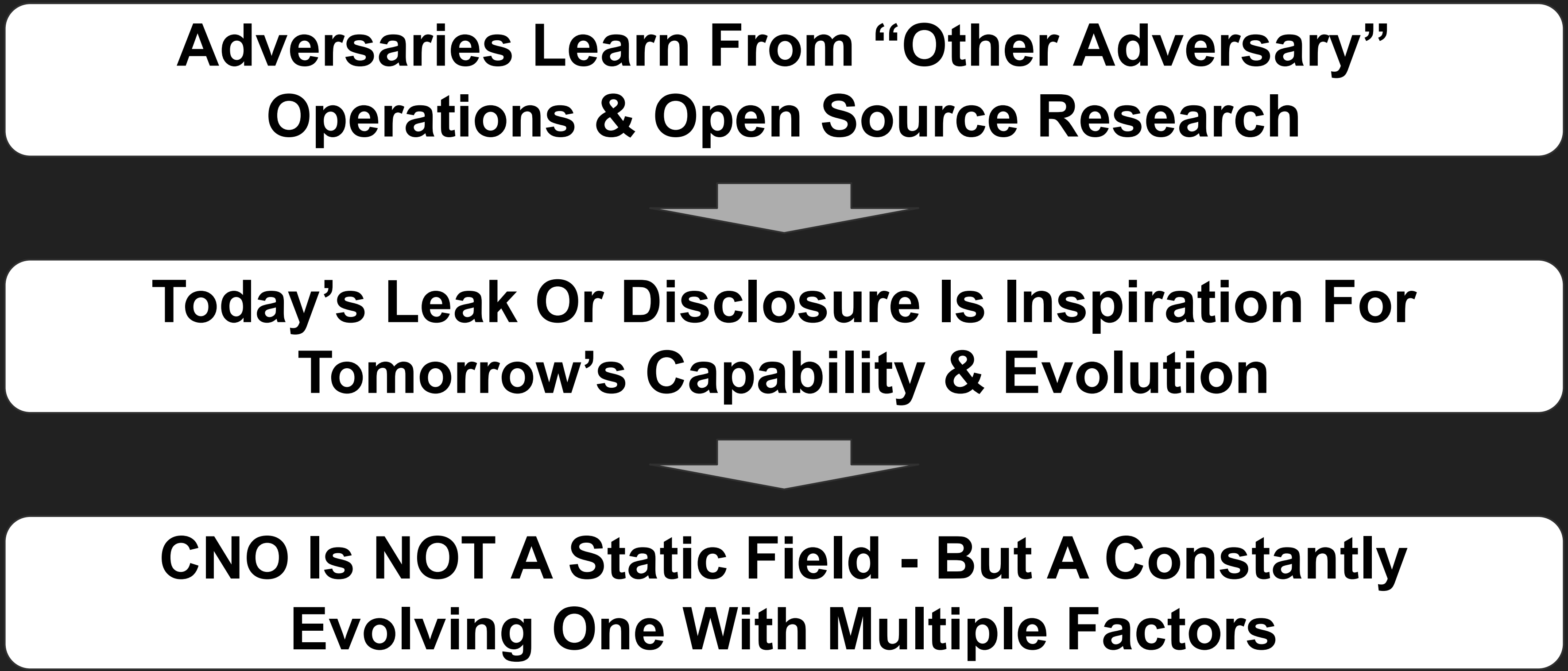
Adversaries Learn From “Other Adversary” Operations & Open Source Research

Capability Inspiration & Proliferation

Adversaries Learn From “Other Adversary” Operations & Open Source Research

Today’s Leak Or Disclosure Is Inspiration For Tomorrow’s Capability & Evolution

Capability Inspiration & Proliferation



Adversaries Learn From “Other Adversary” Operations & Open Source Research

Today’s Leak Or Disclosure Is Inspiration For Tomorrow’s Capability & Evolution

CNO Is NOT A Static Field - But A Constantly Evolving One With Multiple Factors

Guidance For Defenders

Guidance For Defenders

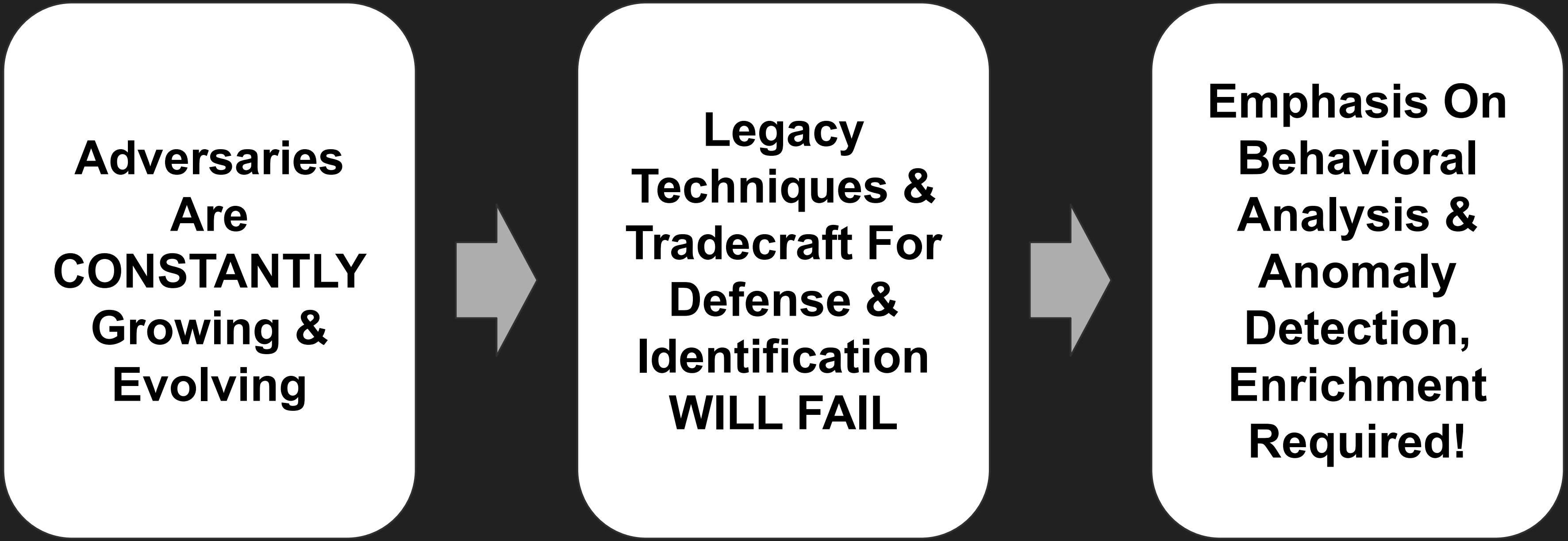
Adversaries Are CONSTANTLY Growing & Evolving

Guidance For Defenders

Adversaries Are CONSTANTLY Growing & Evolving

Legacy Techniques & Tradecraft For Defense & Identification WILL FAIL

Guidance For Defenders



Adversaries Are CONSTANTLY Growing & Evolving

Legacy Techniques & Tradecraft For Defense & Identification WILL FAIL

Emphasis On Behavioral Analysis & Anomaly Detection, Enrichment Required!

Guidance For Defenders

If Adversaries Are Moving Towards Greater Automation & Efficiencies, Defenders Will Be LOST If We Do Not Do The Same!

Advice For Offense

Advice For Offense

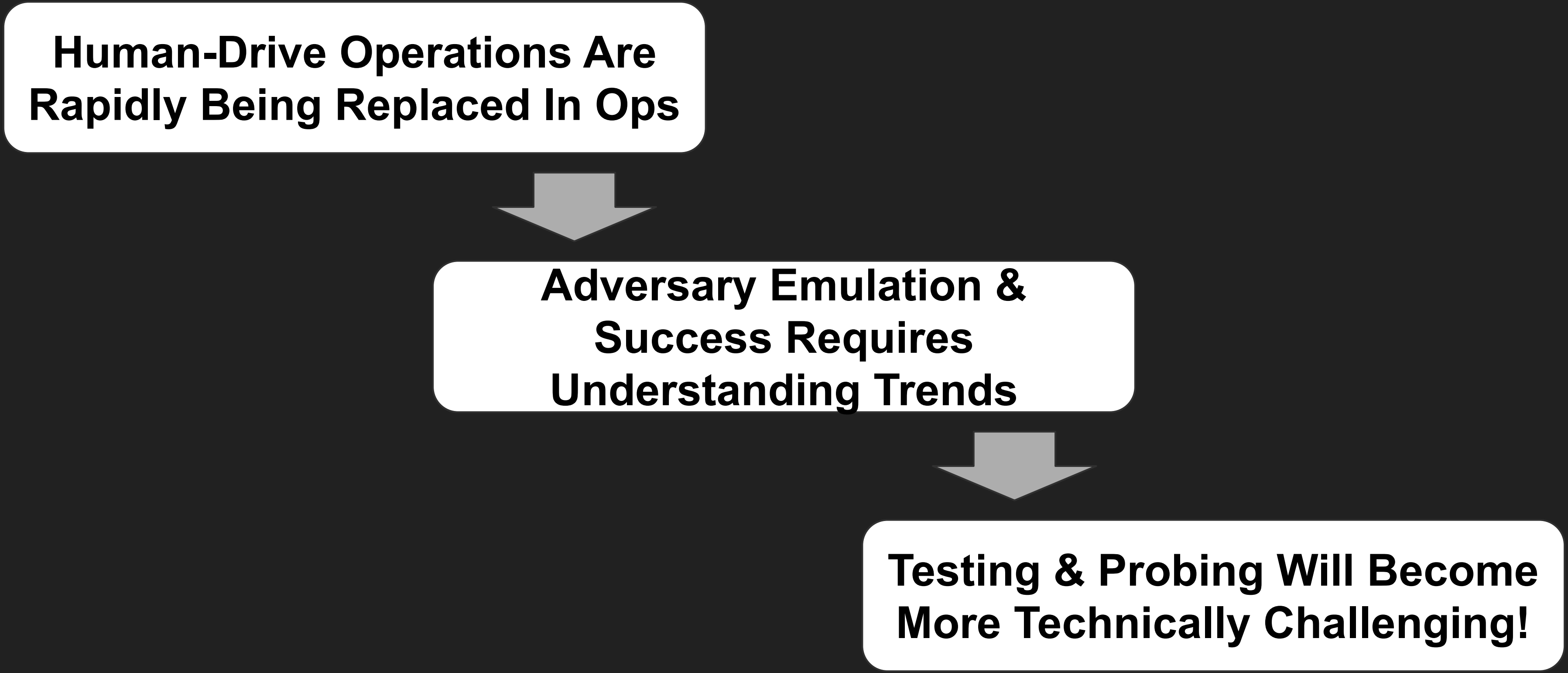
Human-Drive Operations Are Rapidly Being Replaced In Ops

Advice For Offense

Human-Drive Operations Are Rapidly Being Replaced In Ops

Adversary Emulation & Success Requires Understanding Trends

Advice For Offense



Human-Drive Operations Are Rapidly Being Replaced In Ops

Adversary Emulation & Success Requires Understanding Trends

Testing & Probing Will Become More Technically Challenging!

Where Do We Go From Here?

Networks Of Various Types Will Continue To Be Weaponized By Diverse Parties, Either As End-Targets Or Means To Reaching Them…

Where Do We Go From Here?

Networks Of Various Types Will Continue To Be Weaponized By Diverse Parties, Either As End-Targets Or Means To Reaching Them…

…The Increasing Scale & Velocity Of Campaigns Will Make Defense & Response Challenging - But Not Impossible!

Questions?

Selected Works Cited

- The Vulkan Files - Papertrail Media (https://www.papertrailmedia.de/investigations/vulkan-files/)
- Vulkan Files - Der Spiegel (https://www.spiegel.de/thema/vulkanfiles/)
- “Secret Trove Offers Rare Look Into Russian Cyberwar Ambitions” - Craig Timberg, Ellen Nakashima, Hannes Munzinger, & Hakan Tanriverdi, The Washington Post (https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/)
- “‘Vulkan Files’ Leak Reveals Putin’s Global And Domestic Cyberwarfare Tactics” - Luke Harding, Stiliyana Simeonova, Manisha Ganguly, & Dan Sabbagh, The Guardian (https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics)
- “Contracts Identify Cyber Operations Projects From Russian Company NTC Vulkan” - Alden Wahlstrom, Gabby Roncone, Keith Lunden, & Daniel Kapellmann Zafra, Mandiant (https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan)
- “Dragos Analyzes Russian Programs Threatening Critical Civilian Infrastructure” - Kevin Woolf & Bryce Livingston, Dragos (https://hub.dragos.com/hubfs/Dragos_IntelBrief_Russian-Programs-Threatening-Critical_Infrastructure.pdf)
- “Zeroing In On XENOTIME” - Joe Slowik, VirusBulletin (https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Zeroing-in-on-XENOTIME-analysis-of-the-entities-responsible-for-the-Triton-event.pdf)
- CyberWatchers Twitter Thread (https://threadreaderapp.com/thread/1615358254409986053.html)
- “New VPNFilter Malware Targets At Least 500k Networking Devices Worldwide” - William Largent, Cisco Talos (https://blog.talosintelligence.com/vpnfilter/)
- “New Sandworm Malware Cyclops Blink Replaces VPNFilter” - US CISA (https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-054a)
- “The Great Firewall Of China: Xi Jinping’s Internet Shutdown” - Elizabeth C. Economy, The Guardian (https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown)
- “China’s Great Cannon” - Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ron Deibert, & Vern Paxson, The Citizen Lab (https://citizenlab.ca/2015/04/chinas-great-cannon/)
- “A Close Look At The NSA’s Most Powerful Internet Attack Tool” - Nicolas Weaver, Wired (https://www.wired.com/2014/03/quantum/)
- “NSA’s Automated Hacking Engine Offers Hands-Free Pwning Of The World” - Sean Gallagher, Ars Technica (https://arstechnica.com/information-technology/2014/03/nsas-automated-hacking-engine-offers-hands-free-pwning-of-the-world/)
- “Hack Like The NSA: The Quantum Insert” - otw, HackersArise (https://www.hackers-arise.com/post/2016/09/09/hack-like-the-nsa-the-quantum-insert)

Contact Info:

- *joe@paralus.co*
- *@jfslowik - X/Mastodon/Bsky*
- *Signal (Talk To Me First!)*