

# HUNT & HACKETT

OUTSMART YOUR  
DIGITAL ADVERSARIES

---

Attribution in Cyberspace



# About me

- TU Delft Mathematics
- Netherlands Forensic Institute
- AIVD (Dutch Intelligence)
- Fox-IT Cyber Security
- TIB (Oversight of Intelligence Operations)
- Hunt & Hackett: Stopping Digital Espionage



# Definition

Attribution can be broadly defined as the process of assigning responsibility for a (malicious) cyber activity to a specific actor on the basis of the available evidence, including all-source intelligence, forensic investigation, and taking into account the political context. Given the sensitive nature of such evidence and the implications that a decision about attribution might have on bilateral relations between the accuser and the accused, states maintain their exclusive right to attribute (or not) a cyber operation based on their own methods, procedures and political interests.

# Goals of Attribution

- Persons behind an attack
- Motivations of these persons
- Ultimate sponsor of the Attack
- Prepare or Prevent next Attack
- (Cyber) Reaction





NOS Nieuws • Maandag 12 april 2021, 12:00 •  
Aangepast maandag 12 april 2021, 13:49



## 'Kaas-hack' opgelost, ging om gijzelsoftware

# The Dutch were a secret U.S. ally in war against Russian hackers, local media reveal



By [Rick Noack](#)

January 26, 2018 at 8:13 a.m. EST



de Volkskrant



## Hackers AIVD leverden cruciaal bewijs over Russische inmenging in Amerikaanse verkiezingen

Digitale agenten van de AIVD infiltreren in de zomer van 2014 in de beruchte Russische hackgroep Cozy Bear. Ze zien zo als eersten hoe Russische hackers in verkiezingstijd doelen in de VS bestoken: de Democratische Partij, het ministerie van Buitenlandse Zaken en zelfs het Witte Huis. Het is cruciaal bewijs en aanleiding voor de FBI om een onderzoek te beginnen.

Huib Modderkolk 26 januari 2018, 17:00

# **The Netherlands considers Russia's GRU responsible for cyber attacks against Georgia**

Diplomatic statement | 20-02-2020

The Netherlands shares the assessment of Georgia and international partners that the unwarranted large-scale and disruptive cyber attacks against Georgia that took place on 28 October 2019 were carried out by the GRU, Russia's military intelligence service.

The attacks resulted in widespread defacement of websites, including sites belonging to the Georgian government, courts, NGOs, media and businesses. These disruptive operations also interrupted the service of several national broadcasters. The GRU undermined Georgia's sovereignty and disrupted the lives of ordinary Georgian people.

These actions transgress the norms of responsible state behaviour in cyberspace, as agreed upon by the United Nations, and show contempt for the international rules-based order.

We will continue to strengthen resilience in the digital domain, for example by furthering our international cyber capacity building efforts. We are committed to working with all stakeholders to promote accountability in the digital domain.



# WANTED BY THE FBI

## APT 10 GROUP

**Conspiracy to Commit Computer Intrusions; Conspiracy to Commit Wire Fraud;  
Aggravated Identity Theft**



ZHU HUA



ZHANG SHILONG

### DETAILS

On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted ZHU HUA, aka "Afwar," aka "CVNX," aka "Alayos," aka "Godkiller," and ZHANG SHILONG, aka "Baobeilong," aka "Zhang Jianguo," aka "Atreexp," two members of a hacking group operating in China known in the cybersecurity community as Advanced Persistent Threat 10 (the "APT 10 Group"), with conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft. The defendants worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China, and they acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.





The  
Intercept\_



BECOME  
A MEMBER

## THE INSIDE STORY OF HOW BRITISH SPIES HACKED BELGIUM'S LARGEST TELCO

The British government infected Belgacom with among the most advanced malware ever seen.

Belgacom Attack

# Britain's GCHQ Hacked Belgian Telecoms Firm

A cyber attack on Belgacom raised considerable attention last week. Documents leaked by Edward Snowden and seen by SPIEGEL indicate that Britain's GCHQ intelligence agency was responsible for the attack.

20.09.2013, 10.02 Uhr

# TOP SECRET STRAP 2

## One Month Later – OP SOCIALIST

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles



**NAC**  
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation.

[HOME](#) > [BIZ](#) > [ECONOMIE](#)

## ‘Regering zal gepaste stappen ondernemen bij cyberspionage’

16/09/2013 om 10:01 door jvt



# DigiNotar attack



# Attribution by deduction

While Fox-IT did not accuse the Iranian government of conducting or sponsoring the attack, it made clear the motivation behind what it called "Operation Black Tulip."

"The list of domains and the fact that 99% of the users are in Iran suggest that the objective of the hackers is to intercept private information in Iran," the company said in its report.

Some security researchers have suspected that Iran's government was behind the certificate theft and subsequent attack since news broke a week ago. The Fox-IT report only reinforced their beliefs.

# False Flag operations



INDEPENDENT

ENHANCED |

NEWS

SPORT

VOICES

CULTURE

LIFESTYLE

TRAVEL

PREMIUM

MORE

INI

News > World > Europe

## French TV network TV5Monde 'hacked by cyber caliphate in unprecedented attack' that revealed personal details of French soldiers

Messages on the broadcaster's Facebook page purported to show IDs and CVs of relatives of French soldiers

# CYBERCALIPHATE

## Je su**IS** IS



**TV5MONDE**   
Réseau de télévision

 Regarder la vidéo

 J'aime

 Message



Journal

À propos

Photos

TV5MONDE+

Plus +



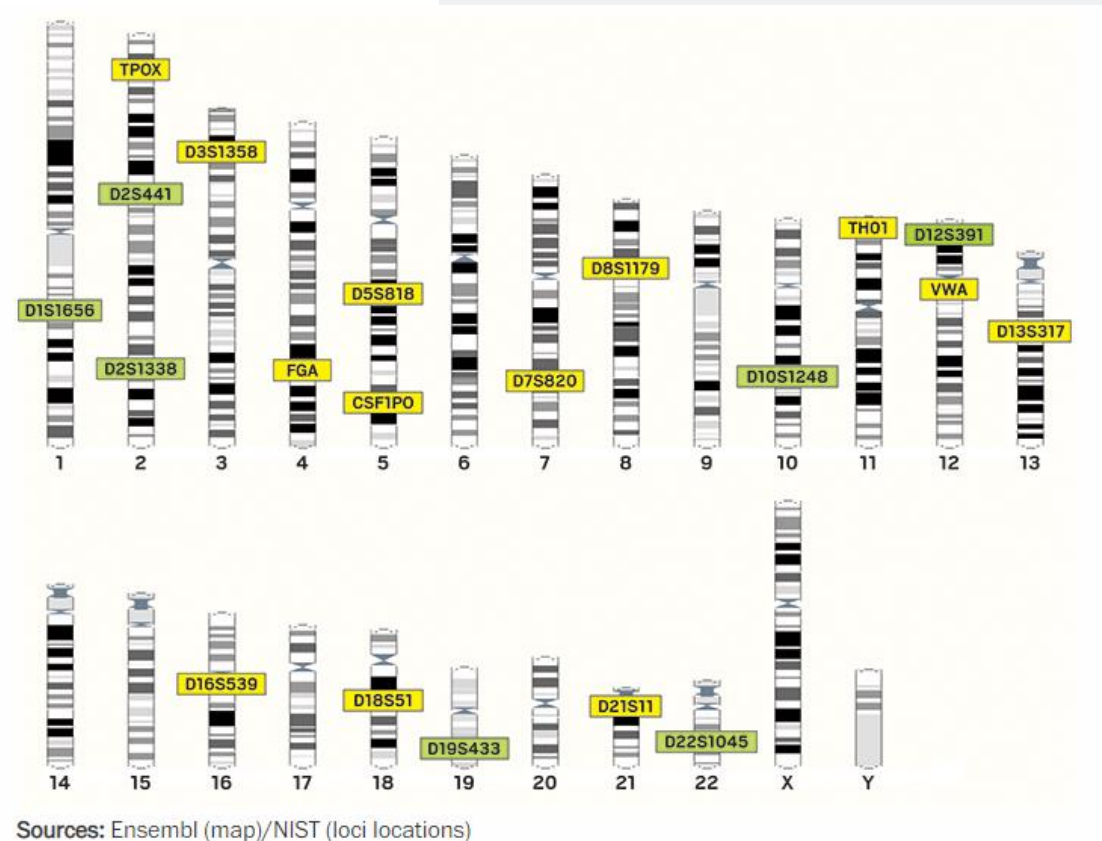


In London, the conclusion was that it was most likely an attempt to test forms of cyber-weaponry as part of an increasingly aggressive posture.

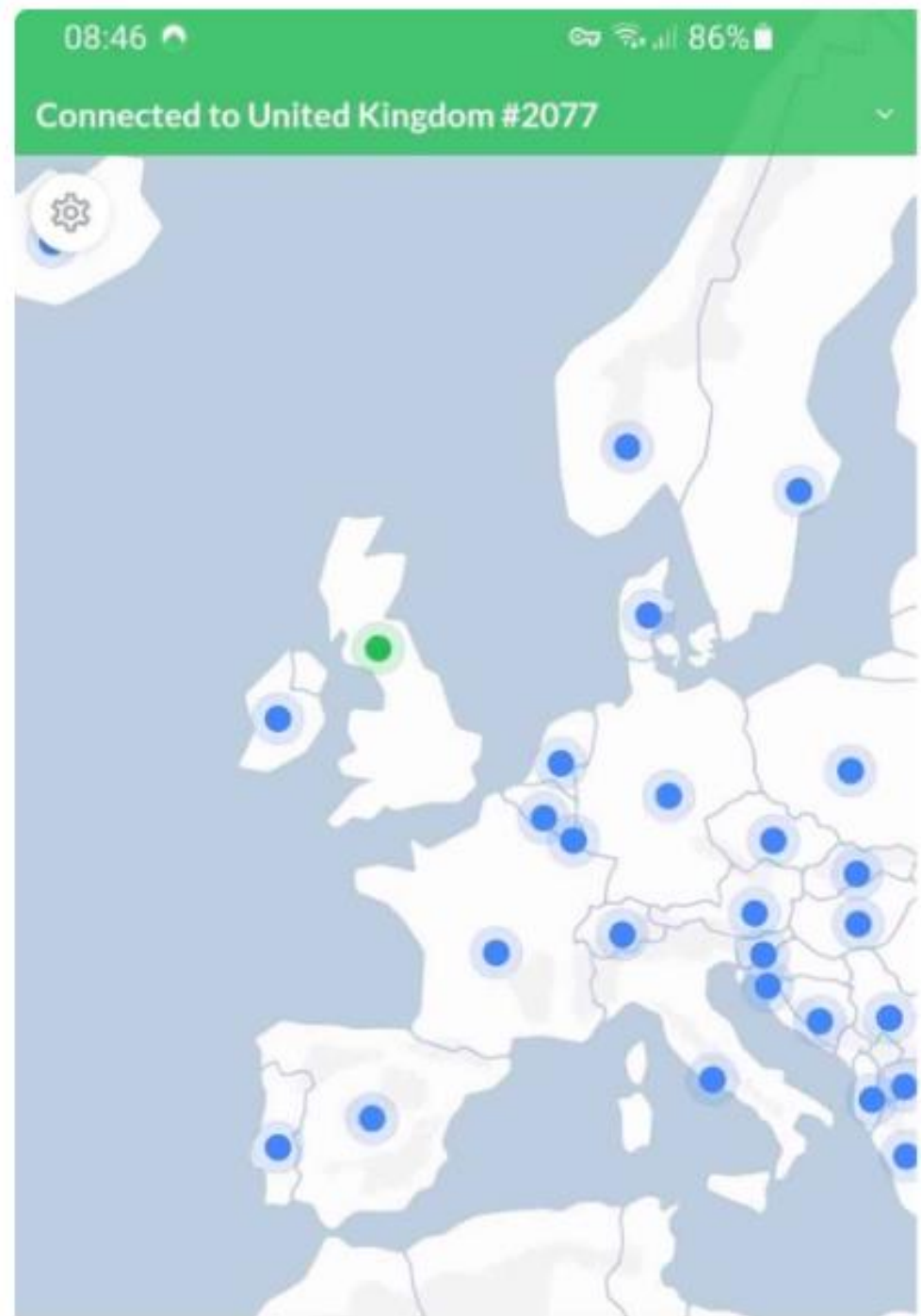
Tech

# How France's TV5 was almost destroyed by 'Russian hackers'

# Why is cyber attribution so difficult?



IP addresses won't  
work



# New law for Dutch Intelligence Services

## Artikel 5

1. Bij een verzoek om toestemming als bedoeld in artikel 45, derde lid, juncto eerste lid, onder b, van de Wiv 2017 blijft het bepaalde in artikel 45, vierde lid, aanhef en onder a, van de Wiv 2017 buiten toepassing.
2. In aanvulling op het bepaalde in artikel 45, achtste lid, van de Wiv 2017, omvat de verleende toestemming tevens de bevoegdheid om, voor de duur van de verleende toestemming, binnen te dringen in een ander geautomatiseerd werk dat door de desbetreffende persoon of organisatie in gebruik is voor zover dat in de plaats treedt van of een aanvulling is op het geautomatiseerde werk waar oorspronkelijk de toestemming voor is verleend.
3. Van de toepassing van het tweede lid wordt terstond mededeling gedaan aan de afdeling toezicht.



# Safeguarding against attack methods

## ATTACK METHODS USED BY THE APTS FOCUSED ON A SECTOR

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 32 techniques	Credential Access 14 techniques	Discovery 23 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Phishing (3/3)	Command and Scripting Interpreter (6/7)	External Remote Services	Valid Accounts (2/3)	Obfuscated Files or Information (5/5)	OS Credential Dumping (5/8)	System Information Discovery	Lateral Tool Transfer	Archive Collected Data (3/3)	Application Layer Protocol (4/4)	Exfiltration Over C2 Channel	System Shutdown/Reboot
External Remote Services	Windows Management Instrumentation	Valid Accounts (2/3)	Process Injection (2/11)	Masquerading (5/6)	Credentials from Password Stores (1/5)	File and Directory Discovery	Exploitation of Remote Services	Data from Local System	Ingress Tool Transfer	Automated Exfiltration (0/0)	Data Destruction
Valid Accounts (2/3)	Exploitation for Client Execution	Office Application Startup (3/6)	Exploitation for Privilege Escalation	Valid Accounts (2/3)	Brute Force (3/4)	System Owner/User Discovery	Internal Spearphishing	Screen Capture	Non-Standard Port	Data Transfer Size Limits	Data Encrypted for Impact
Drive-by Compromise	Shared Modules	Account Manipulation (1/2)	Abuse Elevation Control Mechanism (0/4)	Deobfuscate/Decode Files or Information	Network Sniffing	Process Discovery	Replication Through Removable Media	Automated Collection	Web Service (3/3)	Exfiltration Over Alternative Protocol (0/3)	Resource Hijacking
Exploit Public-Facing Application	Native API	BITS Jobs	Access Token Manipulation (0/5)	Modify Registry	Forced Authentication	System Network Configuration Discovery (0/1)	Software Deployment Tools	Clipboard Data	Proxy (3/4)	Exfiltration Over Other Network Medium (0/1)	Network Denial of Service (0/2)
Trusted Relationship	Software Deployment Tools	Browser Extensions	Boot or Logon Autostart Execution (0/14)	Process Injection (2/11)	Exploitation for Credential Access	Permission Groups Discovery (2/2)	Taint Shared Content	Data from Network Shared Drive	Fallback Channels	Scheduled Transfer	Service Stop
Replication Through Removable Media	Inter-Process Communication (0/2)	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Template Injection	Forge Web Credentials (0/2)	Remote System Discovery	Remote Service Session Hijacking (0/2)	Data from Removable Media	Remote Access Software	Exfiltration Over Physical Medium (0/1)	Account Access Removal
Hardware Additions	Scheduled Task/Job (0/6)	Compromise Client Software Binary	Create or Modify System Process (0/4)	BITS Jobs	Input Capture (0/4)	Software Discovery (1/1)	Remote Services (0/6)	Video Capture	Data Obfuscation (2/3)	Exfiltration Over Web Service (0/2)	Data Manipulation (0/3)
Supply Chain Compromise (0/3)	System Services (0/2)	Create Account (0/2)	Domain Policy Modification (0/2)	Rootkit	Man-in-the-Middle (0/2)	System Network Connections Discovery	Use Alternate Authentication Material (0/2)	Audio Capture	Multi-Stage Channels	Disk Wipe (0/2)	Defacement (0/2)
	User Execution (0/2)	Create or Modify System Process (0/4)	Escape to Host	Exploitation for Defense Evasion	Modify Authentication Process (0/3)	Network Service Scanning		Data from Information Repositories (0/1)	Non-Application Layer Protocol	Endpoint Denial of Service (0/4)	Firmware Corruption
		Event Triggered Execution (0/15)	Event Triggered Execution (0/15)	Abuse Elevation Control Mechanism (0/4)	Steal or Forge Kerberos Tickets (0/4)	Query Registry		Data Staged (0/2)	Communication Through Removable Media	Inhibit System Recovery	
		Hijack Execution Flow (0/11)	Hijack Execution Flow (0/11)	Access Token Manipulation (0/5)	Steal Web Session Cookie	Network Share Discovery		Email Collection (0/3)	Data Encoding (0/2)		
		Modify Authentication Process (0/3)	Scheduled Task/Job (0/6)	Direct Volume Access	Two-Factor Authentication Interception	System Service Discovery		Input Capture (0/4)	Dynamic Resolution (0/3)		
		Pre-OS Boot (0/3)		Domain Policy Modification (0/2)	Unsecured Credentials (0/5)	Network Sniffing		Man in the Browser	Encrypted Channel (0/2)		
		Scheduled Task/Job (0/6)		Execution Guardrails (0/1)		Peripheral Device Discovery		Man-in-the-Middle (0/2)	Traffic Signaling (0/1)		
				File and Directory Permissions Modification (0/2)		Application Window Discovery					
				Hide Artifacts (0/7)		Password Policy Discovery					
				Hijack Execution Flow (0/11)		System Time Discovery					
						Account Discovery (0/3)					

# 122 HOLIDAYS & CELEBRATIONS

*to celebrate in 2022*

## JANUARY

- 1 New Year's Day
- 6 Epiphany (Christian)
- 14 International Kite Festival (India)
- 14 Makar Sankranti (Hindu)\*
- 17 Kid Inventor's Day
- 26 Australia Day (Australia)
- 28 International Lego Day

## FEBRUARY

- 1 Chinese New Year\*
- 1 Lantern Festival (Taiwan)\*
- 1 Black History Month begins (USA)
- 2 Candlemas (Christian)
- 4 Winter Olympics 2022 begin\*
- 5 Sapporo Snow Festival (Japan)\*
- 6 Waitangi Day (New Zealand)
- 12 Carnevale di Venezia (Italy)\*
- 14 Valentine's Day
- 17 Random Acts of Kindness Day
- 27 International Polar Bear Day

## MARCH

- 1 St David's Day (Wales)
- 1 Shrove Tuesday (Christian)\*
- 3 Hinamatsuri (Japan)
- 3 World Wildlife Day
- 8 International Women's Day
- 14 Pi Day
- 17 St Patrick's Day
- 18 Holi (Hindu)\*
- 20 World Storytelling Day
- 21 World Poetry Day
- 22 World Water Day

## APRIL

- 1 April Fool's Day
- 2 International Children's Book Day
- 2 Ramadan begins (Islamic)\*
- 5 Qingming Festival (China)\*
- 13 Songkran begins (Thailand)
- 15 Good Friday (Christian)\*
- 17 Easter Sunday (Christian)\*
- 22 Earth Day
- 23 St George's Day (Europe)
- 23 Çocuk Bayramı (Turkey)
- 25 Anzac Day (Australia & New Zealand)
- 27 King's Day (Netherlands)

## MAY

- 1 May Day
- 1 Vappu (Finland)
- 2 Eid al-Fitr begins (Islamic)\*
- 4 Star Wars Day
- 5 Cinco de Mayo (Mexico)
- 5 Kodomo No Hi (Japan)
- 15 International Day of Families
- 16 Total Eclipse of the Moon\*
- 20 World Bee Day

## JUNE

- 3 Dragon Boat Festival (China)\*
- 3 World Bicycle Day
- 5 World Environment Day
- 8 World Oceans Day
- 18 International Picnic Day
- 19 Juneteenth (USA)
- 20 World Refugee Day
- 21 World Music Day
- 22 World Rainforest Day
- 24 Inti Raymi (Peru)
- 24 Matariki (New Zealand)\*
- 29 International Mud Day

## JULY

- 1 Canada Day (Canada)
- 1 International Joke Day
- 3 NAIDOC Week (Australia)\*
- 4 Independence Day (USA)
- 8 Calgary Stampede (Canada)\*
- 10 Eid al-Adha (Islamic)\*
- 11 Naadam Festival (Mongolia)\*
- 14 Bastille Day (France)
- 30 International Day of Friendship

## AUGUST

- 1 World Wide Web Day
- 11 Raksha Bandhan (Hindu)\*
- 13 Obon (Buddhist)\*
- 13 Left-Handers Day
- 14 Esala Perahera (Buddhist)\*
- 18 Krishna Janmashtami (Hindu)\*
- 19 World Photography Day
- 21 World Senior Citizen's Day
- 26 International Pet Day
- 31 La Tomatina (Spain)\*

## SEPTEMBER

- 5 International Day of Charity
- 6 Read a Book Day (USA)
- 8 International Literacy Day
- 10 Mid-Autumn (Moon) Festival (East & South East Asia)\*
- 21 International Day of Peace
- 25 Rosh Hashanah (Jewish)\*
- 29 Michaelmas (Christian)
- 29 World Maritime Day

## OCTOBER

- 1 Albuquerque International Balloon Fiesta (USA)\*
- 4 World Space Week begins
- 4 World Animal Day
- 4 Yom Kippur (Jewish)\*
- 5 World Teacher's Day
- 10 World Mental Health Day
- 16 World Food Day
- 16 Dictionary Day (USA)
- 24 United Nations Day
- 24 Diwali (Hindu)\*
- 31 Halloween

## NOVEMBER

- 2 Día de Muertos (Mexico)\*
- 5 Guy Fawkes Night (UK)
- 8 Yi Peng Lantern Festival (Thailand)\*
- 11 St Martin's Day (Europe)
- 11 Remembrance Day
- 11 World Origami Day
- 13 World Kindness Day
- 15 Shichi-Go-San (Japan)
- 17 Take a Hike Day (USA)
- 20 Universal Children's Day
- 24 Thanksgiving (USA)\*
- 30 St Andrew's Day (Scotland)

## DECEMBER

- 6 St Nicholas' Day (Europe)
- 7 Día de las Velitas (Colombia)
- 13 St Lucia Day (Europe)
- 16 Las Posadas (Mexico)
- 18 Hanukkah (Jewish)\*
- 24 Jólaflokkur (Iceland)
- 25 Christmas
- 26 Kwaanza (USA)
- 31 New Year's Eve
- 31 Hogmanay (Scotland)

---

# Closing remarks

- Attribution is not something you can do yourself. Most of the time you'll need resources like an intelligence agency has.
- Attribution in cyberspace is very different from the forensics you see in a court of law.
- Intelligence agencies are not willing to share all the evidence. If they share something it will be just the conclusion.
- Nation States use this input for some kind of reaction. 😊



# HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES

RESTRICTED