Case studies in the attribution of cyber operations

Jack Kenny

Post-Doctoral Researcher, Hebrew University of Jerusalem
DPhil Candidate, University of Oxford

Chatham House, 13 January 2020

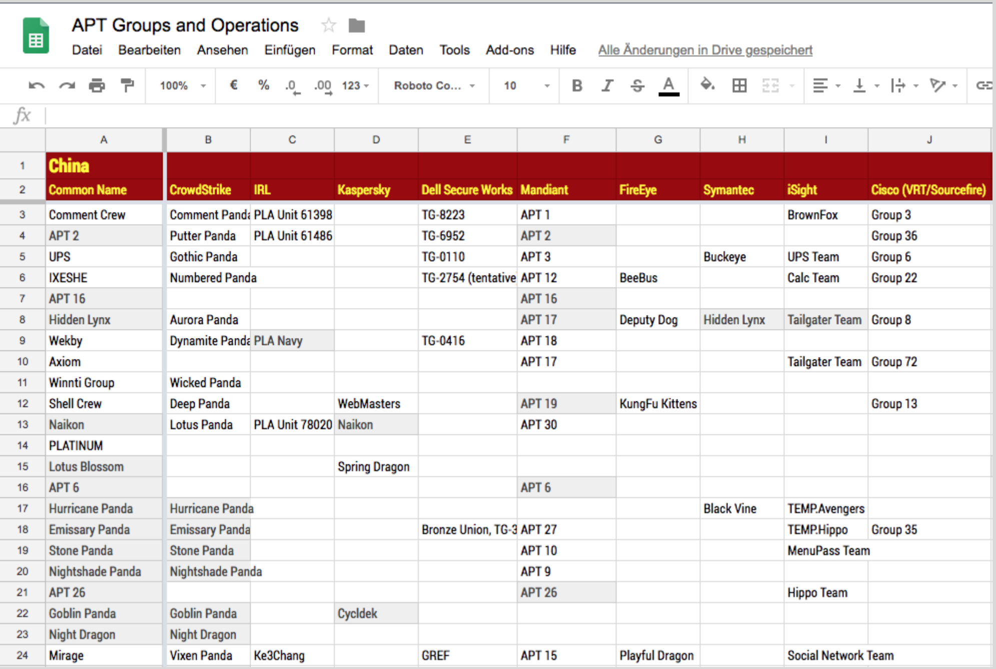
Whitepaper introduction

- Overview and analysis of case studies where states and private companies have made attributions of cyber operations
- Focus of the case studies in attribution on methods/ modality in which attribution is made and attribution under ILC’s ASR

Overview

- Attribution of cyber operations by states
- Co-ordinated state attribution of cyber operations
- State attribution methods/ modalities
- Private sector attribution
- Conclusions

Attribution: what makes cyber operations different?



	A	B	C	D	E	F	G	H	I	J
1	China									
2	Common Name	CrowdStrike	IRL	Kaspersky	Dell Secure Works	Mandiant	FireEye	Symantec	iSight	Cisco (VRT/Sourcefire)
3	Comment Crew	Comment Panda	PLA Unit 61398		TG-8223	APT 1			BrownFox	Group 3
4	APT 2	Putter Panda	PLA Unit 61486		TG-6952	APT 2				Group 36
5	UPS	Gothic Panda			TG-0110	APT 3		Buckeye	UPS Team	Group 6
6	IXESHE	Numbered Panda			TG-2754 (tentative	APT 12	BeeBus		Calc Team	Group 22
7	APT 16					APT 16				
8	Hidden Lynx	Aurora Panda				APT 17	Deputy Dog	Hidden Lynx	Tailgater Team	Group 8
9	Wekby	Dynamite Panda	PLA Navy		TG-0416	APT 18				
10	Axiom					APT 17			Tailgater Team	Group 72
11	Winnti Group	Wicked Panda								
12	Shell Crew	Deep Panda		WebMasters		APT 19	KungFu Kittens			Group 13
13	Naikon	Lotus Panda	PLA Unit 78020	Naikon		APT 30				
14	PLATINUM									
15	Lotus Blossom			Spring Dragon						
16	APT 6					APT 6				
17	Hurricane Panda	Hurricane Panda						Black Vine	TEMP.Avengers	
18	Emissary Panda	Emissary Panda			Bronze Union, TG-3	APT 27			TEMP.Hippo	Group 35
19	Stone Panda	Stone Panda				APT 10			MenuPass Team	
20	Nightshade Panda	Nightshade Panda				APT 9				
21	APT 26					APT 26			Hippo Team	
22	Goblin Panda	Goblin Panda		Cycldek						
23	Night Dragon	Night Dragon								
24	Mirage	Vixen Panda	Ke3Chang		GREF	APT 15	Playful Dragon		Social Network Team	

"APT Groups and Operations" spreadsheet, https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit#gid=1864660085

- ICJ in *Nicaragua* dealt with attribution of non-state actors to a state
- Scale and number of APT groups
- Frequent attacks, continuous basis without physical constraint, often against multiple states simultaneously
- Routed through one or many state territories instantaneously
- Geographical evidence is easily manipulated or hidden, 'false flag' operations

Table 1: Attribution of Cyber Operations by States*

Date	Activity	State attribution	Detail and confidence level	Private sector support	Possible bases for attribution (ILC's Articles on State Responsibility)*
2007	**Estonian DDoS** attacks, attributed to Russian state organs	Initial attribution by Estonia attributed attacks to organs of the Russian state.	Confidence of initial attribution subsequently undermined by further Estonian statement, and later said to be based on 'circumstantial evidence' with 'no direct evidence linking the attacks to the Russian state'.	Unnamed officials and experts in media reports support the attribution of the attack to Russia or Russian state institutions or intelligence services.	Article 4
2012	**DDoS attacks on US banks**, attributed to Iranian state sponsored hackers	US DoJ indictment attributed attacks to 'nation-state sponsored hackers' working for companies that performed work on behalf of the Iranian Government.	US indictment details operation of two companies responsible and their direct links to state, ITSecTeam and Mersad Company. Indictment provides great detail on the role of companies and individuals in the attacks.	Unnamed US official sources in media reports attribute to Iranian hackers with government ties, attacks 'bore signatures' that allowed US investigators to trace attacks back to Iranian government.	Article 5, Article 8
2014	**Sony Pictures**, attributed to Lazarus Group (North Korea)	FBI, in collaboration with other US government department and agencies, attributed attack to North Korean government (2014). 2018 US DoJ indictment attributed attack to the Lazarus group working on behalf of the North Korean government.	US DoJ indictment laid out in great detail that provides context and support in technical evidence that led to the attribution.	There is support from the private sector for the FBI attribution, specifically to attribute the attacks to the Lazarus group, allegedly controlled by Bureau 121, a division of the Reconnaissance General Bureau, a North Korean intelligence agency.	Article 8
2015	**German Parliament**, attributed to Sofacy group (Russia)	Bundesamt für Verfassungsschutz, Germany's domestic intelligence agency, attributed the attack to the Sofacy group, also known as APT 28, who they identified as being managed by Russian secret services.	FireEye: in releasing indicators of compromise, US Government confirmed what FireEye had 'long upheld', that ATP28 is sponsored by the Russian government.	There is additional support from the private sector that supports the Sofacy group being sponsored by the Russian state.	Article 8
2015	**Ukraine power grid** attacks, attributed to Russia-based actors	The attribution of the attack to Russian special services by the Security Service of Ukraine was performed quickly.	Ukrainian investigation supported by US agencies and has further support from a general statement of attribution of the attacks to Russia from the US.	FireEye attributed the attacks to 'Russian-nexus actors'.	Article 4
2016	**Bangladesh Central Bank**, attributed to Lazarus group (North Korea)	US DoJ indictment attributed to the Lazarus group working on behalf of the North Korean government.	179-page indictment laid out in great detail that provides context and support in technical evidence that led to the attribution.	Significant support from private sector reports to indicate the Lazarus group were responsible. Lazarus group linked by Symantec to North Korea, while Kaspersky: 'direct connection' between North Korea and Lazarus.	Article 8

* DISCLAIMER: This table is based on attribution statements by states and the private sector. Whether the evidence relied on by those states and private sector actors in making those attribution statements is sufficient to meet the thresholds of attribution under the corresponding Articles of State Responsibility often cannot be established from open source information.

Table 2: Coordinated State Attribution of Cyber Operations*

Date	Activity	International attribution	Detail and confidence level	Private sector support	Possible bases for attribution (ILC's Articles on State Responsibility)*
Dec 17	**Wannacry** ransomware attack attributed to the Lazarus Group (North Korea)	**Attributed**: UK, US, Australia (3) **Supported**: New Zealand, Denmark, Japan (3)	Coordinated joint attribution by states directly attributed attacks to the North Korean state. NCSC: 'highly likely' 'North Korean actors known as the Lazarus Group' responsible. US: Lazarus group 'cyber affiliates of the North Korean government'.	Support from private sector attributing attacks to Lazarus Group. Symantec: 'highly likely' Lazarus group were responsible. FireEye: 'at a minimum, WannaCry operators share software development resources with North Korean espionage operators'.	Article 8
Feb 18	**NotPetya** destructive cyber-attack attributed to Russian military, Russian state-sponsored actors	**Attributed**: UK, US, Australia, Canada, Denmark (5) **Supported**: New Zealand, Estonia, Finland, Latvia, Lithuania, Netherlands, Norway, Sweden (8)	Strong support from multiple states attributing attack with high confidence to the Russian military, and to Russian state-sponsored actors.	Private sector intelligence links attack to Sandworm, group of hackers within the Russian GRU, based on intelligence from firms including FireEye and ESET that shared crucial forensic connections.	Article 4, Article 8
Mar 18	**Universities spear-phishing campaign** attributed to Mabna Institute (Iran)	**Attributed**: UK (criminal actors in Iran), US (IRGC and Iranian government) (2)	The NCSC: 'high confidence' Mabna Institute 'almost certainly responsible'. US indictment: Mabna Institute created 'to assist Iranian universities and scientific and research organisations in stealing access to non-Iranian scientific resources'.	–	Article 8, Article 5
May 18	**Router compromises** attributed to Russian state sponsored actors	**Attributed**: UK, US, Australia (3)	The US and UK governments attributed the malicious cyber activity to 'Russian state-sponsored cyber actors' with 'high confidence'.	–	Article 8
Oct 18	**GRU campaign** of indiscriminate and reckless cyber-attacks, attributed to Russian GRU	**Attributed**: UK, US, Australia, Canada, New Zealand, Netherlands, Germany (7) **Supported**: Czech Republic, Denmark, Estonia, Finland, France, Latvia, Japan, Norway, Poland, Romania, Slovakia, Sweden, Ukraine, EU, NATO (15)	UK NCSC attributes four specific cyber-attacks with 'high confidence' to GRU who were 'almost certainly responsible'. US indictment charged Russian GRU officers for involvement in the attacks. UK and the Netherlands joint statement attributes attacks to GRU. New Zealand's GCSB 'established clear links between the Russian government and a campaign of malicious cyber activity', citing a 'robust attribution process' which 'strongly links four international malicious cyber instances since 2015 to the Russian government'. Australia attributed the operations to 'the Russian military, and their intelligence arm 'the GRU'.	Mandiant and several other private sector firms attribute individual operations, including the DNC hack, to the group known as APT28, acknowledged in the NCSC statement as a group belonging to the GRU.	Article 4, Article 8
Dec 18	**APT10 intrusion set** attributed to APT10 (China)	**Attributed**: UK, US, Australia, Canada, New Zealand (5) **Supported**: Denmark, Estonia, Finland, Germany, Japan, Netherlands, Norway, Poland, Romania, Sweden (10)	NCSC: APT10 'almost certainly' responsible. NCSC: 'highly likely' APR10 has 'enduring relationship with the Chinese Ministry of State Security, and operates to meet Chinese State requirements,' 'Chinese Ministry of State was responsible'. US indictment: two Chinese nationals, members of the APT10 hacking group 'acting in association with the Tianjin State Security Bureau' in series of malicious cyber operations that 'gave China's intelligence service access to sensitive business information'. Australia: attributed attacks to APT10, 'acting on behalf of the Chinese Ministry of State Security'. Canada's CSE: 'almost certain that that actors likely associated with the People's Republic of China Ministry of State Security' were responsible. New Zealand's GCSB 'established links between' the Chinese Ministry of State Security and the campaign of cyber operations.	Further support from private sector reports identify APT10 as a Chinese based espionage group which appear to be working in support of Chinese national security goals, and from media reports based on unnamed government and private sector sources discussing the hacker groups responsible as being directly connected to the Chinese Ministry of State Security.	Article 8
Oct 19	**Turla group exploits Iranian APT** attributed to Russia-based actors	**Attributed**: UK, US (2)	NCSC and NSA joint statement attributes to actor 'suspected to be Russia-based'.	–	Article 8

* DISCLAIMER: This table is based on attribution statements by states and the private sector. Whether the evidence relied on by those states and private sector actors in making those attribution statements is sufficient to meet the thresholds of attribution under the corresponding Articles of State Responsibility often cannot be established from open source information.

State attribution methods/ modalities

- General statements of attribution: political and legal aspects
  - Little/sparse technical analysis or support for findings (outside of private sector attribution reports)
  - Non-specific violations of international law
- Indictments of foreign actors in-absentia

‘These attacks have been conducted *in flagrant violation of international law*, have affected citizens in a large number of countries, including Russia, and have cost national economies millions of pounds.’

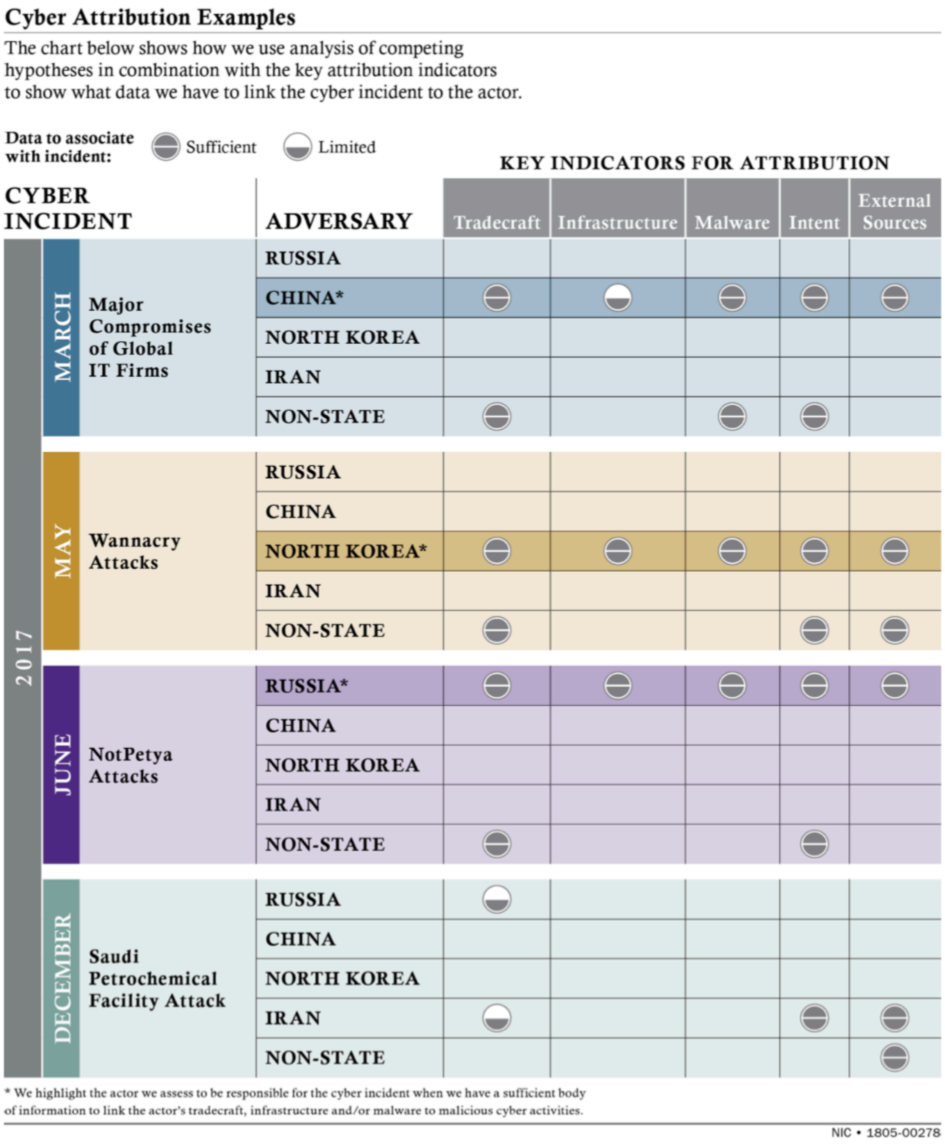
‘Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed’ (*National Cyber Security Centre*, 3 October 2018) <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> accessed 4 June 2019

State attribution methods/ modalities

1. **Key indicators**
2. Confidence levels
3. Classifications of cyber attacks
4. Information and context of assessments

US Office of the Director of National Intelligence (**2018**)

'A Guide to Cyber Attribution' <https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf>



Cyber Attribution Examples

The chart below shows how we use analysis of competing hypotheses in combination with the key attribution indicators to show what data we have to link the cyber incident to the actor.

Data to associate with incident: ● Sufficient ◒ Limited

		CYBER INCIDENT	ADVERSARY	KEY INDICATORS FOR ATTRIBUTION				
				Tradecraft	Infrastructure	Malware	Intent	External Sources
2017	MARCH	Major Compromises of Global IT Firms	RUSSIA					
			CHINA*	●	◒	●	●	●
			NORTH KOREA					
			IRAN					
			NON-STATE	●		●	●	
	MAY	Wannacry Attacks	RUSSIA					
			CHINA					
			NORTH KOREA*	●	●	●	●	●
			IRAN					
			NON-STATE	●			●	●
	JUNE	NotPetya Attacks	RUSSIA*	●	●	●	●	●
			CHINA					
			NORTH KOREA					
			IRAN					
			NON-STATE	●			●	
	DECEMBER	Saudi Petrochemical Facility Attack	RUSSIA	◒				
			CHINA					
			NORTH KOREA					
			IRAN	◒			●	●
			NON-STATE					●

* We highlight the actor we assess to be responsible for the cyber incident when we have a sufficient body of information to link the actor's tradecraft, infrastructure and/or malware to malicious cyber activities.

NIC • 1805-00278

State attribution methods/ modalities

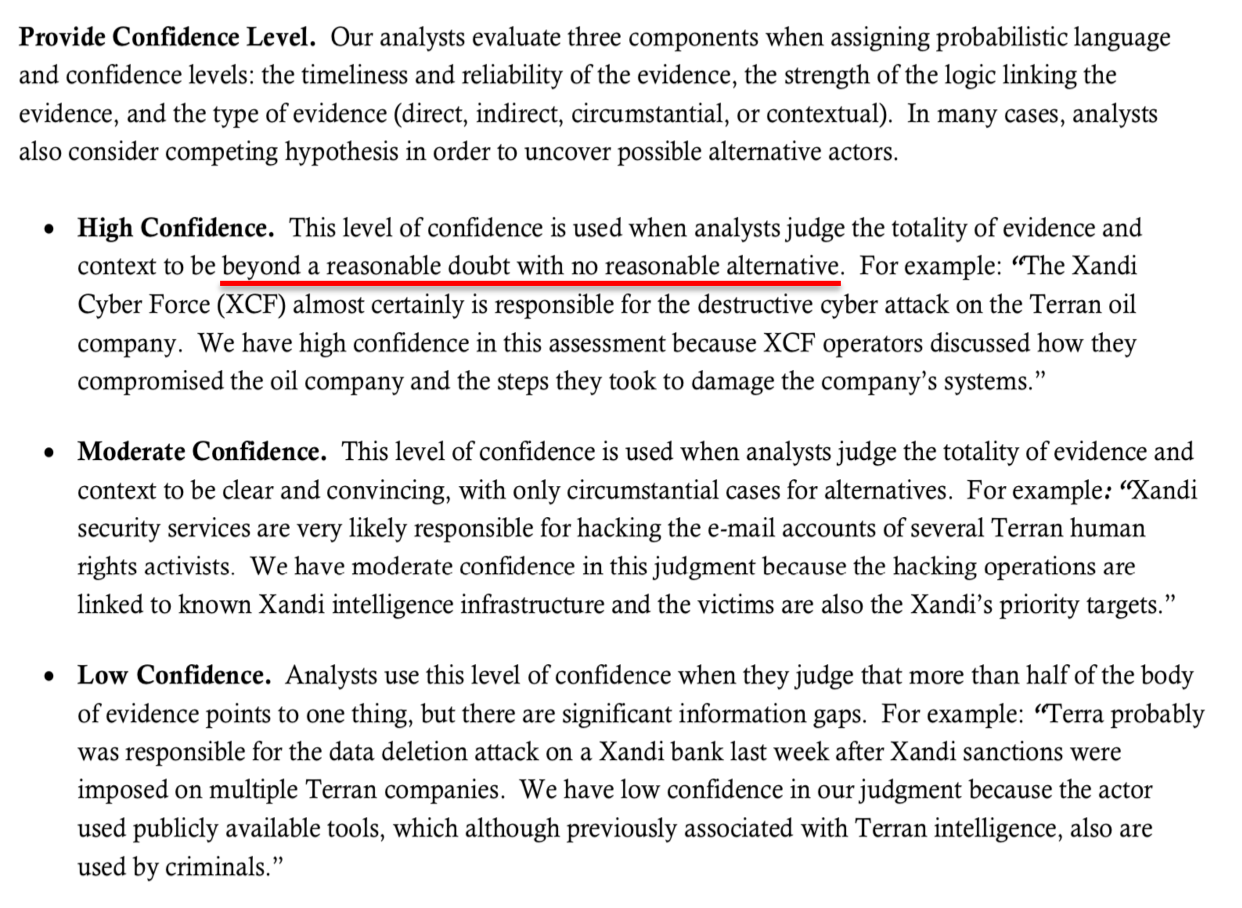
1. **Key indicators**
2. Confidence levels
3. Classifications of cyber attacks
4. Information and context of assessments

- France lists non-exhaustive factors to be taken into account in attributing cyber-attacks to a responsible attacker/ state:
  - Determination of the cyber infrastructure from which the cyberattack originated/ transited and their geographical locations
  - Identification of the modes of operation of the adversary
  - History of activities of the perpetrator
  - Scale and severity of the incident
  - Compromised area and the effects sought by the attacker

'Droit International Appliqué Aux Opérations Dans Le Cyberspace', Ministère des Armées **(2019)**

State attribution methods/ modalities

1. Key indicators
2. **Confidence levels**
3. Classifications of cyber attacks
4. Information and context of assessments



Provide Confidence Level. Our analysts evaluate three components when assigning probabilistic language and confidence levels: the timeliness and reliability of the evidence, the strength of the logic linking the evidence, and the type of evidence (direct, indirect, circumstantial, or contextual). In many cases, analysts also consider competing hypothesis in order to uncover possible alternative actors.

- **High Confidence.** This level of confidence is used when analysts judge the totality of evidence and context to be beyond a reasonable doubt with no reasonable alternative. For example: "The Xandi Cyber Force (XCF) almost certainly is responsible for the destructive cyber attack on the Terran oil company. We have high confidence in this assessment because XCF operators discussed how they compromised the oil company and the steps they took to damage the company's systems."

- **Moderate Confidence.** This level of confidence is used when analysts judge the totality of evidence and context to be clear and convincing, with only circumstantial cases for alternatives. For example*:* "Xandi security services are very likely responsible for hacking the e-mail accounts of several Terran human rights activists. We have moderate confidence in this judgment because the hacking operations are linked to known Xandi intelligence infrastructure and the victims are also the Xandi's priority targets."

- **Low Confidence.** Analysts use this level of confidence when they judge that more than half of the body of evidence points to one thing, but there are significant information gaps. For example: "Terra probably was responsible for the data deletion attack on a Xandi bank last week after Xandi sanctions were imposed on multiple Terran companies. We have low confidence in our judgment because the actor used publicly available tools, which although previously associated with Terran intelligence, also are used by criminals."

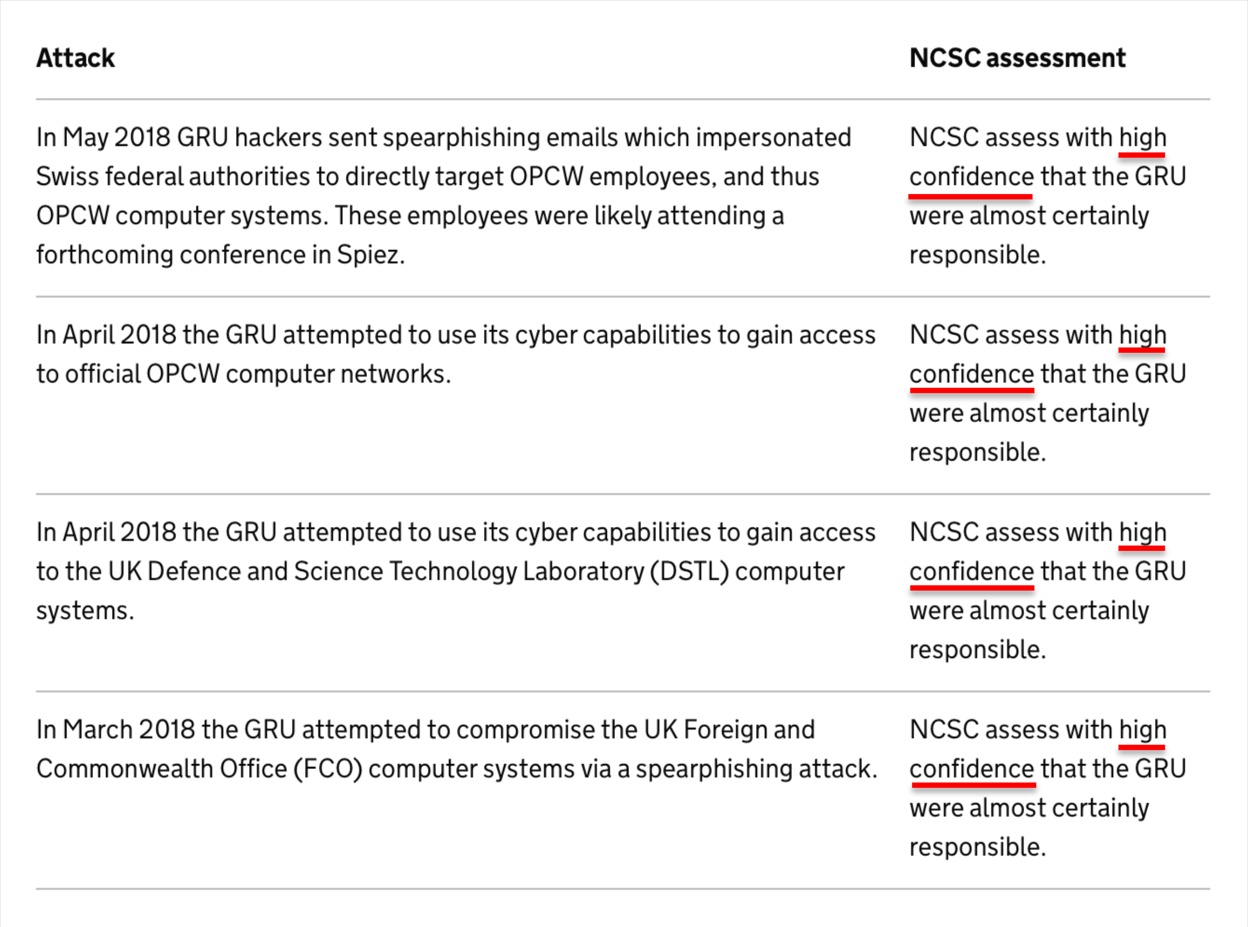
US Office of the Director of National Intelligence (**2018**)

'A Guide to Cyber Attribution' <https://www.dni.gov/files/CTIIC/documents/ODNI_A_Guide_to_Cyber_Attribution.pdf>

State attribution methods/ modalities

1. Key indicators
2. **Confidence levels**
3. Classifications of cyber attacks
4. Information and context of assessments

UK exposes Russian Cyber Attacks (**2018**)

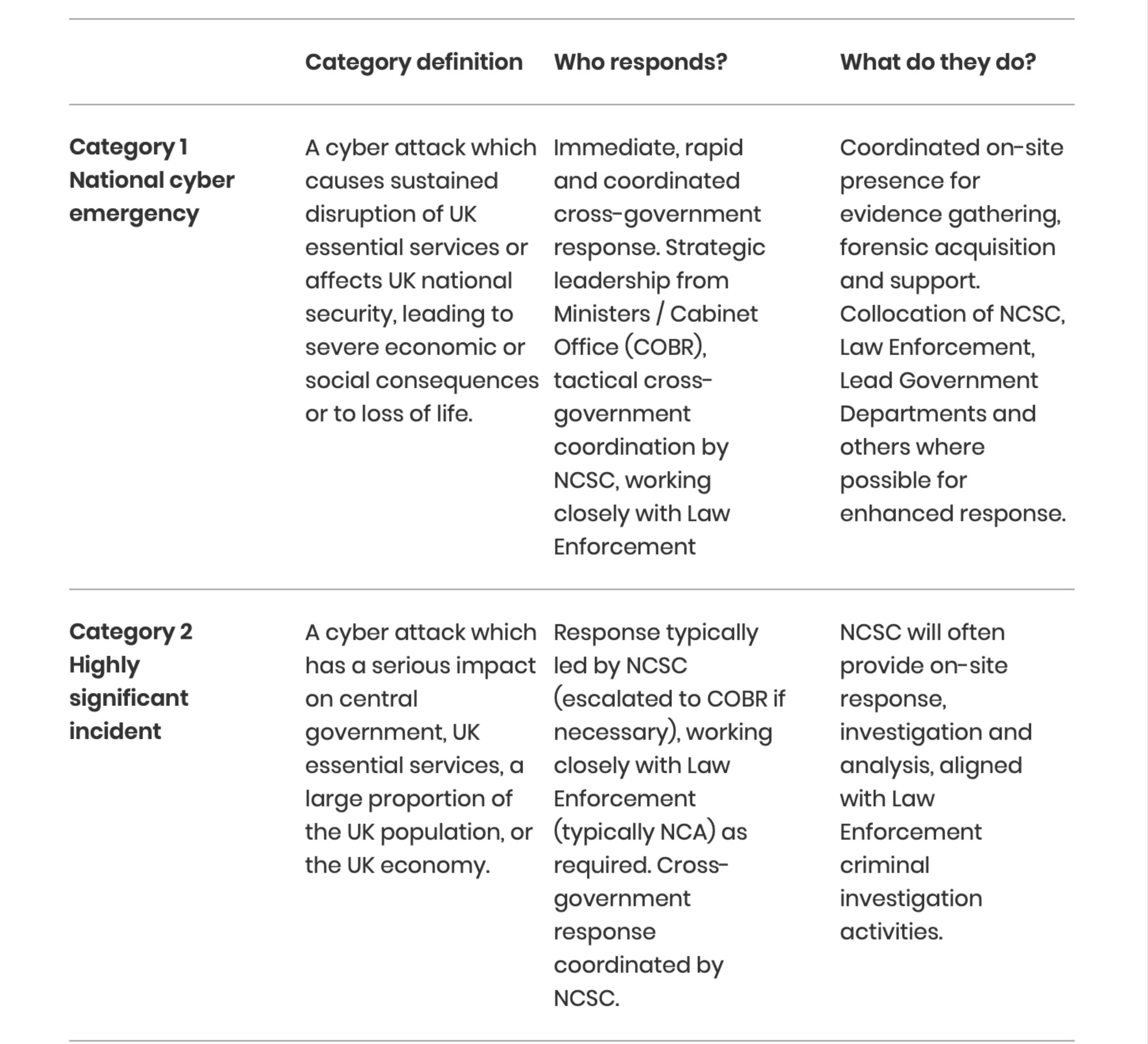


Attack	NCSC assessment
In May 2018 GRU hackers sent spearphishing emails which impersonated Swiss federal authorities to directly target OPCW employees, and thus OPCW computer systems. These employees were likely attending a forthcoming conference in Spiez.	NCSC assess with high confidence that the GRU were almost certainly responsible.
In April 2018 the GRU attempted to use its cyber capabilities to gain access to official OPCW computer networks.	NCSC assess with high confidence that the GRU were almost certainly responsible.
In April 2018 the GRU attempted to use its cyber capabilities to gain access to the UK Defence and Science Technology Laboratory (DSTL) computer systems.	NCSC assess with high confidence that the GRU were almost certainly responsible.
In March 2018 the GRU attempted to compromise the UK Foreign and Commonwealth Office (FCO) computer systems via a spearphishing attack.	NCSC assess with high confidence that the GRU were almost certainly responsible.

'UK Exposes Russian Cyber Attacks' (*GOV.UK*, 4 October 2018) <https://www.gov.uk/government/news/uk-exposes-russian-cyber-attacks

State attribution methods/ modalities

1. Key indicators
2. Confidence levels
3. **Classifications of cyber attacks**
4. Information and context of assessments



	Category definition	Who responds?	What do they do?
Category 1 National cyber emergency	A cyber attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life.	Immediate, rapid and coordinated cross-government response. Strategic leadership from Ministers / Cabinet Office (COBR), tactical cross-government coordination by NCSC, working closely with Law Enforcement	Coordinated on-site presence for evidence gathering, forensic acquisition and support. Collocation of NCSC, Law Enforcement, Lead Government Departments and others where possible for enhanced response.
Category 2 Highly significant incident	A cyber attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.	Response typically led by NCSC (escalated to COBR if necessary), working closely with Law Enforcement (typically NCA) as required. Cross-government response coordinated by NCSC.	NCSC will often provide on-site response, investigation and analysis, aligned with Law Enforcement criminal investigation activities.

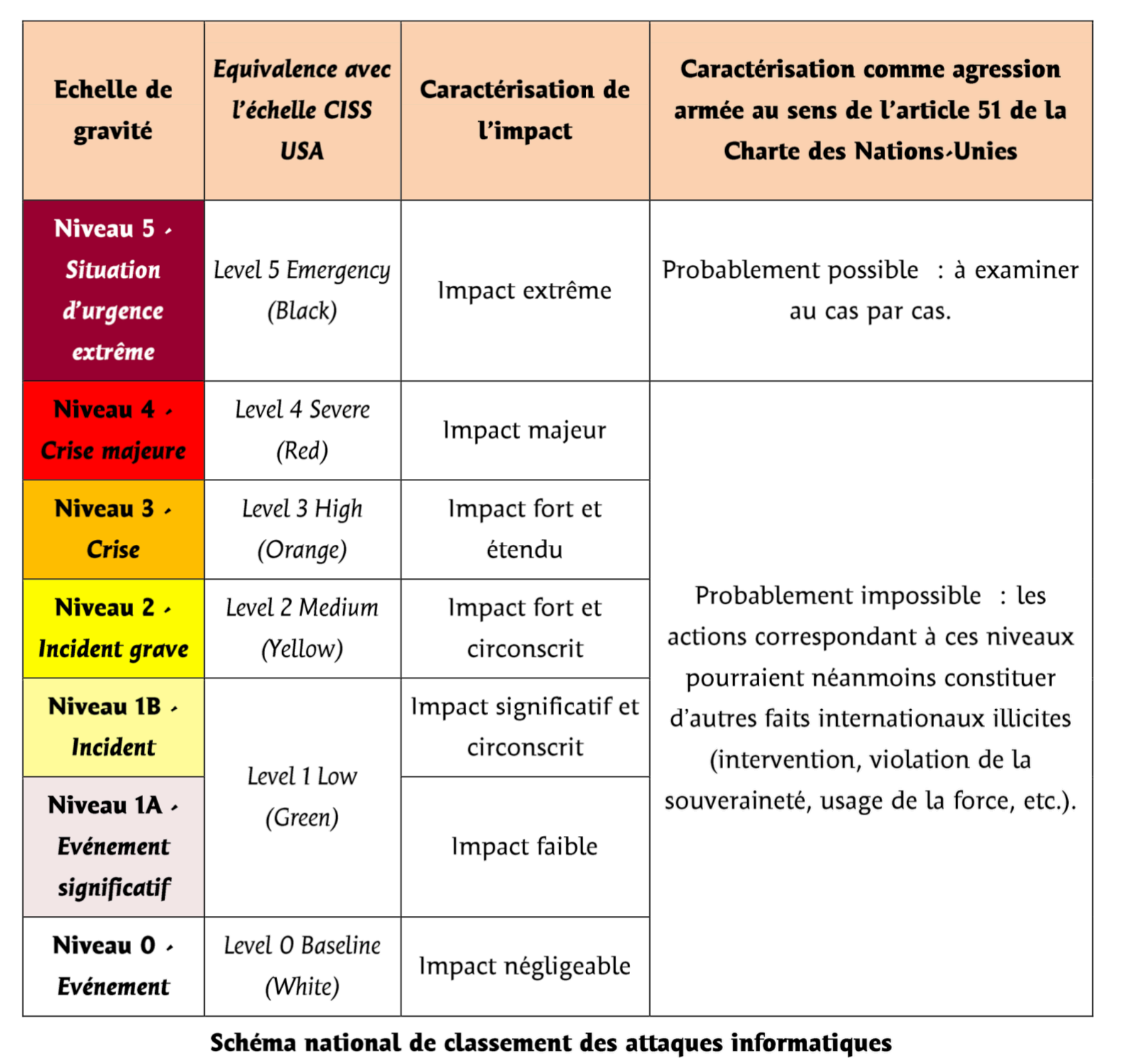
- no C1 level incident- death or serious injury
- C2- 1,500 incidents- majority caused by states

'New Cyber Attack Categorisation System to Improve UK Response to Incidents' (*National Cyber Security Centre*, 11 April **2018**) <https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents>

State attribution methods/ modalities

1. Key indicators
2. Confidence levels
3. **Classifications of cyber attacks**
4. Information and context of assessments

‘Revue Stratégique de Cyberdéfense’ (**2018**) <http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf>



Echelle de gravité	***Equivalence avec l’échelle CISS USA***	**Caractérisation de l’impact**	**Caractérisation comme agression armée au sens de l’article 51 de la Charte des Nations-Unies**
Niveau 5 - ***Situation d’urgence extrême***	*Level 5 Emergency (Black)*	Impact extrême	Probablement possible : à examiner au cas par cas.
Niveau 4 - ***Crise majeure***	*Level 4 Severe (Red)*	Impact majeur	Probablement impossible : les actions correspondant à ces niveaux pourraient néanmoins constituer d’autres faits internationaux illicites (intervention, violation de la souveraineté, usage de la force, etc.).
Niveau 3 - ***Crise***	*Level 3 High (Orange)*	Impact fort et étendu	
Niveau 2 - ***Incident grave***	*Level 2 Medium (Yellow)*	Impact fort et circonscrit	
Niveau 1B - ***Incident***	*Level 1 Low (Green)*	Impact significatif et circonscrit	
Niveau 1A - ***Evénement significatif***		Impact faible	
Niveau 0 - ***Evénement***	*Level 0 Baseline (White)*	Impact négligeable	

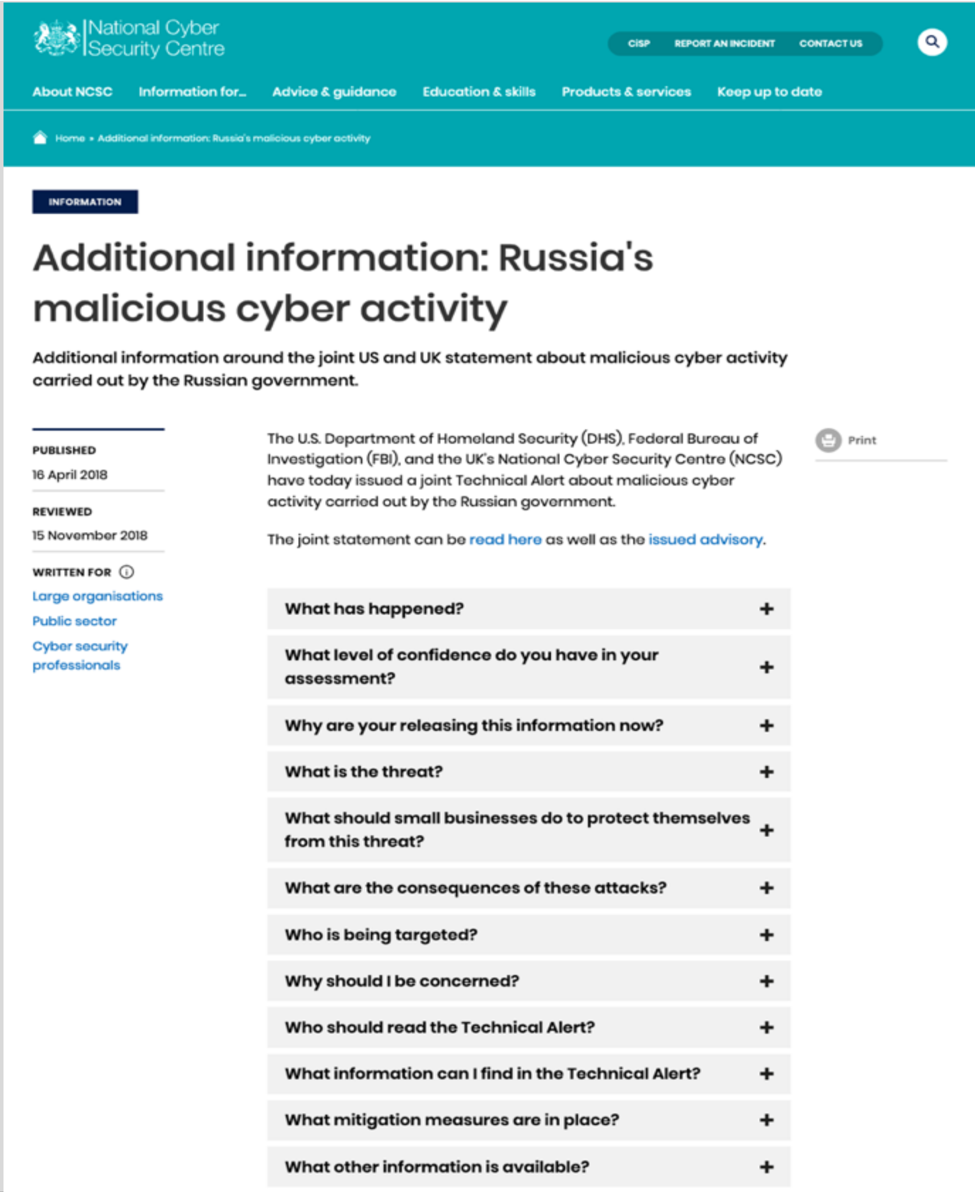
Schéma national de classement des attaques informatiques

State attribution methods/ modalities

1. Key indicators
2. Confidence levels
3. Classifications of cyber attacks
4. **Information and context of assessments**

- Indictments of foreign nationals in-absentia

‘Additional Information: Russia’s Malicious Cyber Activity - NCSC’ https://www.ncsc.gov.uk/information/additional-information-russias-malicious-cyber-activity



Additional information: Russia's malicious cyber activity

Additional information around the joint US and UK statement about malicious cyber activity carried out by the Russian government.

PUBLISHED
16 April 2018

REVIEWED
15 November 2018

WRITTEN FOR
Large organisations
Public sector
Cyber security professionals

The U.S. Department of Homeland Security (DHS), Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Centre (NCSC) have today issued a joint Technical Alert about malicious cyber activity carried out by the Russian government.

The joint statement can be read here as well as the issued advisory.

What has happened? +

What level of confidence do you have in your assessment? +

Why are your releasing this information now? +

What is the threat? +

What should small businesses do to protect themselves from this threat? +

What are the consequences of these attacks? +

Who is being targeted? +

Why should I be concerned? +

Who should read the Technical Alert? +

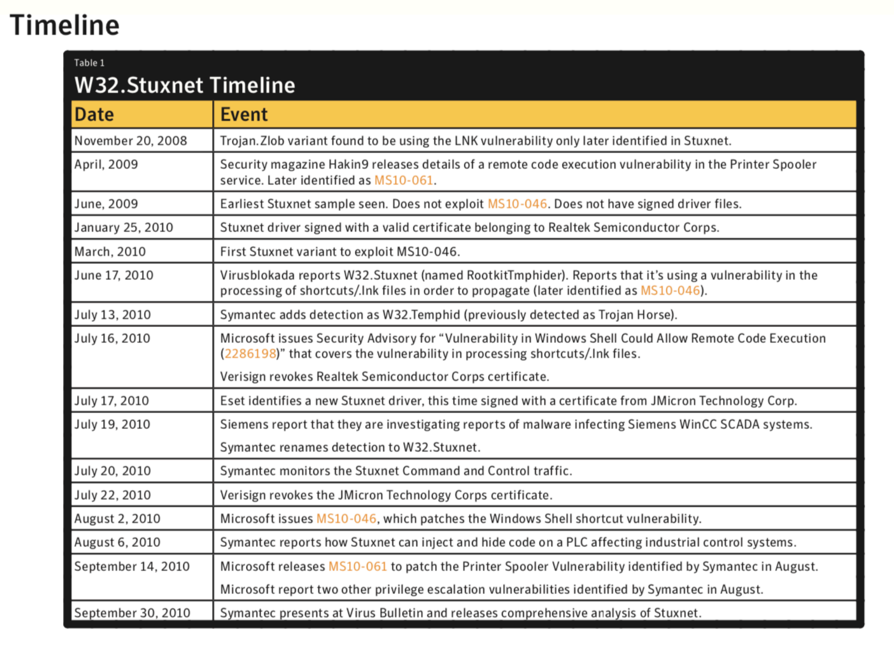
What information can I find in the Technical Alert? +

What mitigation measures are in place? +

What other information is available? +

Value of private sector attribution: Stuxnet (2010)

- Indirect support
- Media, tech
- Different approaches/ perspectives

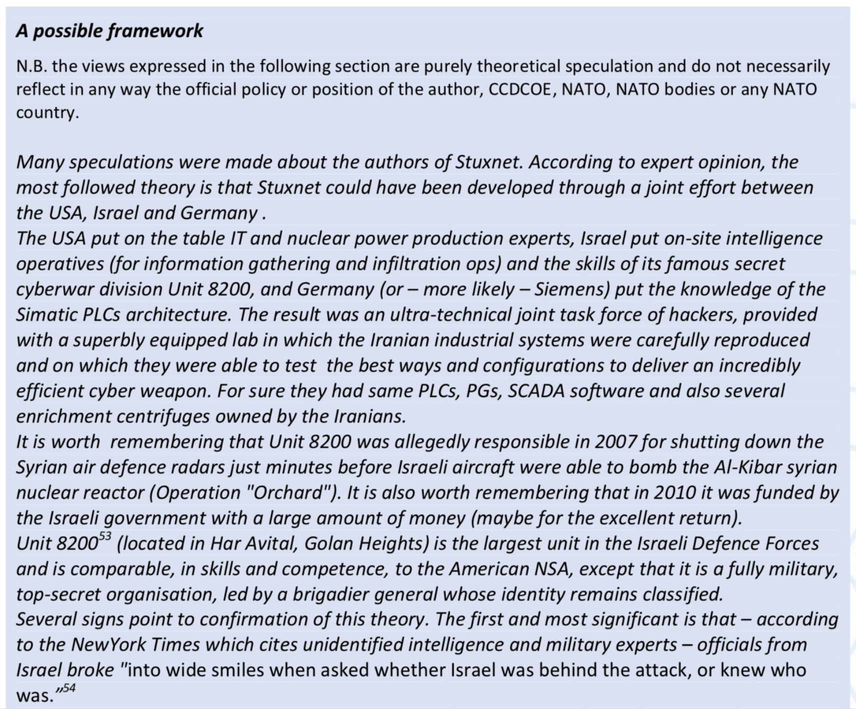


Timeline

Table 1

W32.Stuxnet Timeline

Date	Event
November 20, 2008	Trojan.Zlob variant found to be using the LNK vulnerability only later identified in Stuxnet.
April, 2009	Security magazine Hakin9 releases details of a remote code execution vulnerability in the Printer Spooler service. Later identified as MS10-061.
June, 2009	Earliest Stuxnet sample seen. Does not exploit MS10-046. Does not have signed driver files.
January 25, 2010	Stuxnet driver signed with a valid certificate belonging to Realtek Semiconductor Corps.
March, 2010	First Stuxnet variant to exploit MS10-046.
June 17, 2010	Virusblokada reports W32.Stuxnet (named RootkitTmphider). Reports that it's using a vulnerability in the processing of shortcuts/.lnk files in order to propagate (later identified as MS10-046).
July 13, 2010	Symantec adds detection as W32.Temphid (previously detected as Trojan Horse).
July 16, 2010	Microsoft issues Security Advisory for "Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)" that covers the vulnerability in processing shortcuts/.lnk files. Verisign revokes Realtek Semiconductor Corps certificate.
July 17, 2010	Eset identifies a new Stuxnet driver, this time signed with a certificate from JMicron Technology Corp.
July 19, 2010	Siemens report that they are investigating reports of malware infecting Siemens WinCC SCADA systems. Symantec renames detection to W32.Stuxnet.
July 20, 2010	Symantec monitors the Stuxnet Command and Control traffic.
July 22, 2010	Verisign revokes the JMicron Technology Corps certificate.
August 2, 2010	Microsoft issues MS10-046, which patches the Windows Shell shortcut vulnerability.
August 6, 2010	Symantec reports how Stuxnet can inject and hide code on a PLC affecting industrial control systems.
September 14, 2010	Microsoft releases MS10-061 to patch the Printer Spooler Vulnerability identified by Symantec in August. Microsoft report two other privilege escalation vulnerabilities identified by Symantec in August.
September 30, 2010	Symantec presents at Virus Bulletin and releases comprehensive analysis of Stuxnet.



A possible framework

N.B. the views expressed in the following section are purely theoretical speculation and do not necessarily reflect in any way the official policy or position of the author, CCDCOE, NATO, NATO bodies or any NATO country.

Many speculations were made about the authors of Stuxnet. According to expert opinion, the most followed theory is that Stuxnet could have been developed through a joint effort between the USA, Israel and Germany .

The USA put on the table IT and nuclear power production experts, Israel put on-site intelligence operatives (for information gathering and infiltration ops) and the skills of its famous secret cyberwar division Unit 8200, and Germany (or – more likely – Siemens) put the knowledge of the Simatic PLCs architecture. The result was an ultra-technical joint task force of hackers, provided with a superbly equipped lab in which the Iranian industrial systems were carefully reproduced and on which they were able to test the best ways and configurations to deliver an incredibly efficient cyber weapon. For sure they had same PLCs, PGs, SCADA software and also several enrichment centrifuges owned by the Iranians.

It is worth remembering that Unit 8200 was allegedly responsible in 2007 for shutting down the Syrian air defence radars just minutes before Israeli aircraft were able to bomb the Al-Kibar syrian nuclear reactor (Operation "Orchard"). It is also worth remembering that in 2010 it was funded by the Israeli government with a large amount of money (maybe for the excellent return).

Unit 8200[53] (located in Har Avital, Golan Heights) is the largest unit in the Israeli Defence Forces and is comparable, in skills and competence, to the American NSA, except that it is a fully military, top-secret organisation, led by a brigadier general whose identity remains classified.

Several signs point to confirmation of this theory. The first and most significant is that – according to the NewYork Times which cites unidentified intelligence and military experts – officials from Israel broke "into wide smiles when asked whether Israel was behind the attack, or knew who was."[54]

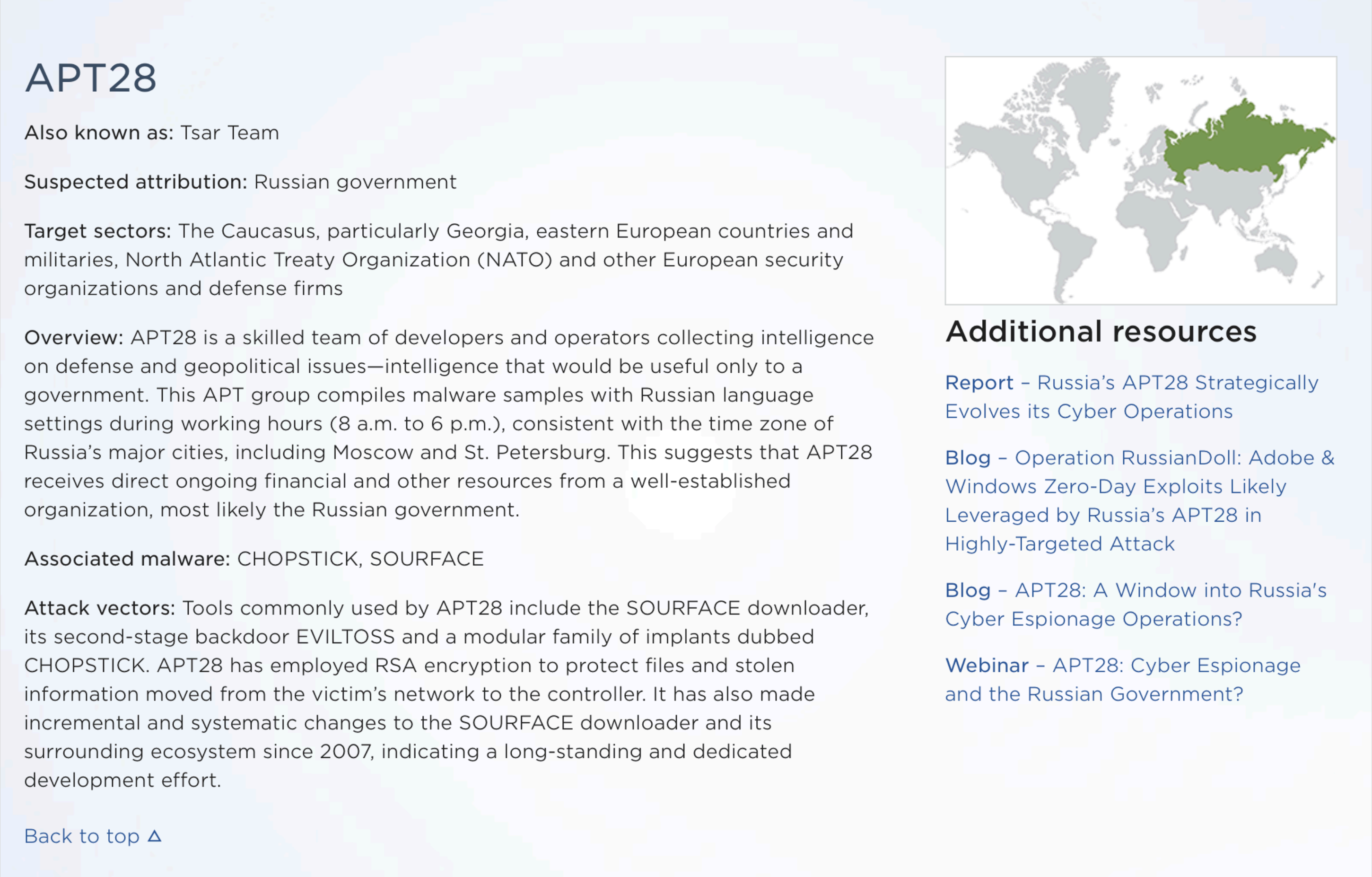
- **Technical**

W32.Stuxnet Dossier Version 1.4, Symantec Security Response (2011)

- **Political**

CCD COE *Stuxnet Facts Report: A Technical and Strategic Analysis* (2012)

Private sector profiling of APT groups



APT28

Also known as: Tsar Team

Suspected attribution: Russian government

Target sectors: The Caucasus, particularly Georgia, eastern European countries and militaries, North Atlantic Treaty Organization (NATO) and other European security organizations and defense firms

Overview: APT28 is a skilled team of developers and operators collecting intelligence on defense and geopolitical issues—intelligence that would be useful only to a government. This APT group compiles malware samples with Russian language settings during working hours (8 a.m. to 6 p.m.), consistent with the time zone of Russia's major cities, including Moscow and St. Petersburg. This suggests that APT28 receives direct ongoing financial and other resources from a well-established organization, most likely the Russian government.

Associated malware: CHOPSTICK, SOURFACE

Attack vectors: Tools commonly used by APT28 include the SOURFACE downloader, its second-stage backdoor EVILTOSS and a modular family of implants dubbed CHOPSTICK. APT28 has employed RSA encryption to protect files and stolen information moved from the victim's network to the controller. It has also made incremental and systematic changes to the SOURFACE downloader and its surrounding ecosystem since 2007, indicating a long-standing and dedicated development effort.

Back to top △

Additional resources

Report – Russia's APT28 Strategically Evolves its Cyber Operations

Blog – Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack

Blog – APT28: A Window into Russia's Cyber Espionage Operations?

Webinar – APT28: Cyber Espionage and the Russian Government?

https://www.fireeye.com/current-threats/apt-groups.html

Table 2: Coordinated State Attribution of Cyber Operations*

Date	Activity	International attribution	Detail and confidence level	Private sector support	Possible bases for attribution (ILC's Articles on State Responsibility)*
Dec 17	**Wannacry** ransomware attack attributed to the Lazarus Group (North Korea)	**Attributed**: UK, US, Australia (3) **Supported**: New Zealand, Denmark, Japan (3)	Coordinated joint attribution by states directly attributed attacks to the North Korean state. NCSC: 'highly likely' 'North Korean actors known as the Lazarus Group' responsible. US: Lazarus group 'cyber affiliates of the North Korean government'.	Support from private sector attributing attacks to Lazarus Group. Symantec: 'highly likely' Lazarus group were responsible. FireEye: 'at a minimum, WannaCry operators share software development resources with North Korean espionage operators'.	Article 8
Feb 18	**NotPetya** destructive cyber-attack attributed to Russian military, Russian state-sponsored actors	**Attributed**: UK, US, Australia, Canada, Denmark (5) **Supported**: New Zealand, Estonia, Finland, Latvia, Lithuania, Netherlands, Norway, Sweden (8)	Strong support from multiple states attributing attack with high confidence to the Russian military, and to Russian state-sponsored actors.	Private sector intelligence links attack to Sandworm, group of hackers within the Russian GRU, based on intelligence from firms including FireEye and ESET that shared crucial forensic connections.	Article 4, Article 8
Mar 18	**Universities spear-phishing campaign** attributed to Mabna Institute (Iran)	**Attributed**: UK (criminal actors in Iran), US (IRGC and Iranian government) (2)	The NCSC: 'high confidence' Mabna Institute 'almost certainly responsible'. US indictment: Mabna Institute created 'to assist Iranian universities and scientific and research organisations in stealing access to non-Iranian scientific resources'.	–	Article 8, Article 5
May 18	**Router compromises** attributed to Russian state sponsored actors	**Attributed**: UK, US, Australia (3)	The US and UK governments attributed the malicious cyber activity to 'Russian state-sponsored cyber actors' with 'high confidence'.	–	Article 8
Oct 18	**GRU campaign** of indiscriminate and reckless cyber-attacks, attributed to Russian GRU	**Attributed**: UK, US, Australia, Canada, New Zealand, Netherlands, Germany (7) **Supported**: Czech Republic, Denmark, Estonia, Finland, France, Latvia, Japan, Norway, Poland, Romania, Slovakia, Sweden, Ukraine, EU, NATO (15)	UK NCSC attributes four specific cyber-attacks with 'high confidence' to GRU who were 'almost certainly responsible'. US indictment charged Russian GRU officers for involvement in the attacks. UK and the Netherlands joint statement attributes attacks to GRU. New Zealand's GCSB 'established clear links between the Russian government and a campaign of malicious cyber activity', citing a 'robust attribution process' which 'strongly links four international malicious cyber instances since 2015 to the Russian government'. Australia attributed the operations to 'the Russian military, and their intelligence arm 'the GRU'.	Mandiant and several other private sector firms attribute individual operations, including the DNC hack, to the group known as APT28, acknowledged in the NCSC statement as a group belonging to the GRU.	Article 4, Article 8
Dec 18	**APT10 intrusion set** attributed to APT10 (China)	**Attributed**: UK, US, Australia, Canada, New Zealand (5) **Supported**: Denmark, Estonia, Finland, Germany, Japan, Netherlands, Norway, Poland, Romania, Sweden (10)	NCSC: APT10 'almost certainly' responsible. NCSC: 'highly likely' APR10 has 'enduring relationship with the Chinese Ministry of State Security, and operates to meet Chinese State requirements,' 'Chinese Ministry of State was responsible'. US indictment: two Chinese nationals, members of the APT10 hacking group 'acting in association with the Tianjin State Security Bureau' in series of malicious cyber operations that 'gave China's intelligence service access to sensitive business information'. Australia: attributed attacks to APT10, 'acting on behalf of the Chinese Ministry of State Security'. Canada's CSE: 'almost certain that that actors likely associated with the People's Republic of China Ministry of State Security' were responsible. New Zealand's GCSB 'established links between' the Chinese Ministry of State Security and the campaign of cyber operations.	Further support from private sector reports identify APT10 as a Chinese based espionage group which appear to be working in support of Chinese national security goals, and from media reports based on unnamed government and private sector sources discussing the hacker groups responsible as being directly connected to the Chinese Ministry of State Security.	Article 8
Oct 19	**Turla group exploits Iranian APT** attributed to Russia-based actors	**Attributed**: UK, US (2)	NCSC and NSA joint statement attributes to actor 'suspected to be Russia-based'.	–	Article 8

* DISCLAIMER: This table is based on attribution statements by states and the private sector. Whether the evidence relied on by those states and private sector actors in making those attribution statements is sufficient to meet the thresholds of attribution under the corresponding Articles of State Responsibility often cannot be established from open source information.

Observations

- Trend: Western states coordinate attributions of cyber-attacks to increase legitimacy and strengthen accountability
- Private sector attribution reports: indirect support for state attributions
- Attribution of attack to APT group vs attribution of APT group to a state
  - Lack of open source information?
  - Unclear language, statements conflate two steps
  - Inconsistent nomenclature of APT groups
  - Break down sustained campaigns into specific attributions
- Adopt and find common ground to develop standardised usage
  - Key indicators
  - Confidence levels in attribution
  - Classifications/ categorisations of cyber-attacks
  - Information and context for the performance of attributions
  - Maintaining APT profiles and attack databases
- Microsoft CyperPeace Institute

Thank you

jack.kenny@law.ox.ac.uk