RSAConference2020
Asia Pacific & Japan

A Virtual Learning Experience | 15–17 July

HUMAN ELEMENT

SESSION ID: **AIR-F03**

When World News Matters to You: Operationalizing Geopolitical Intelligence

Mei Nelson

Security Innovation Principal
Accenture Security / iDefense
@mei8nelson

May 12, 2019:


Questions swirl over 'sabotage attack' as Iran tensions ratchet up
Oil Tankers Attacked Off United Arab Emirates
UAE says four ships subjected to 'sabotage' off east coast
UAE tanker attacks blamed on 'state actor'
Failed U.S.-Iran Diplomacy Sets Stage for New Spike in Tensions

Questions

- CEO asks the CISO
  - What should we worry about?
- CISO asks the SOC manager
  - What are you seeing?
- SOC manager asks the analyst:
  - What are you looking for?

Geopolitical Intelligence

- Understanding a threat environment from military, political, economic, social, and cultural perspectives
- Putting threats in context

Geopolitical Intelligence Helps to Answer

- What in the world happened, based on facts not speculation?
- Who are the players involved?
- Why do the players do what they do?
- When and what are the players going to do in response?
- How is it likely to affect us?

RSAConference2020 APJ
A Virtual Learning Experience

How Geopolitical Intelligence Reinforces Cyberdefense Operations

Cyber Threat Intelligence

"Cyber threat intelligence is simply information about threats and threat actors that provides sufficient understanding for mitigating a harmful event in the cyber domain."

- CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations

Cyber Threat Intelligence Drives Three Levels of Cyberdefense

- Strategic level
  - Organization-level cyberdefense vision, policies, strategies, and investments to achieve the organization's mission and goals
- Operational level
  - Designing and managing defense team organizational structure and SOPs
  - Planning and carrying out system, tool and information source procurement and development
  - Practicing incident response drills and implementing striated and role-based information control measures
- Tactical level
  - Crafting threat hunting signatures and intrusion detection system alerts
  - Blocking malicious or suspicious traffic at a firewall

How Cyber Threat Intelligence Drives Three Levels of Cyberdefense

- Strategic level
  - Identities, motivations, intentions, locations, capabilities, limitations of threats and their sponsors, etc.
- Operational level
  - Threat actor tactics, techniques, and procedures (TTPs), defining how much and what data to gather, significant calendar dates, etc.
- Tactical level
  - Malicious IP addresses, domains, file hashes, email senders, etc.

Geopolitical Intelligence Informs Cyber Threat Intelligence

Strategic: CEO, COO, CFO

- Apportioning security investment
- Realigning organization priorities
- Assessing risks of organizational changes
- Evaluating market changes
- Developing high-level capability
- Assessing country-related risks

Operational: CISO, CIO, Risk Manager

- Calibrating threat models
- Operational decisions
- Overcome stove piping
- Employee education
- Operational procedures

TACTICAL/OPERATIONAL

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Motivation	Open Source Intelligence	Public Relations, Reputation for prosecuting		Public Relations		
Objectives	Web analytics, Open Source Intelligence			OPSEC	Public Relations	
Avenue of approach	Web / Network analytics		Dynamic Defense	Dynamic Defense, OPSEC	Direct towards stronger defenses	
Capability	Open Source Intelligence		Insider threat program	Dynamic Defense	Direct towards stronger defenses	
Access	Open Source Intelligence, web/network analytics	Insider threat program		Dynamic Defense, OPSEC		
Actions	Insider threat program, Supply chain awareness, Intel-driven CND	Role based access		Quality of Service	Honeypot	
Assess	Web analytics, Social Media	Public Relations			Public Relations, Honeypot	
Restrike	Web / Network analytics, Open Source Intelligence,	Dynamic Defense			Public Relations, Honeypot	

Source: "Operational Levels of Cyber Intelligence," September 2013, Intelligence and National Security Alliance

Using Threat Actor-focused Intelligence

RSAConference2020 APJ

A Virtual Learning Experience

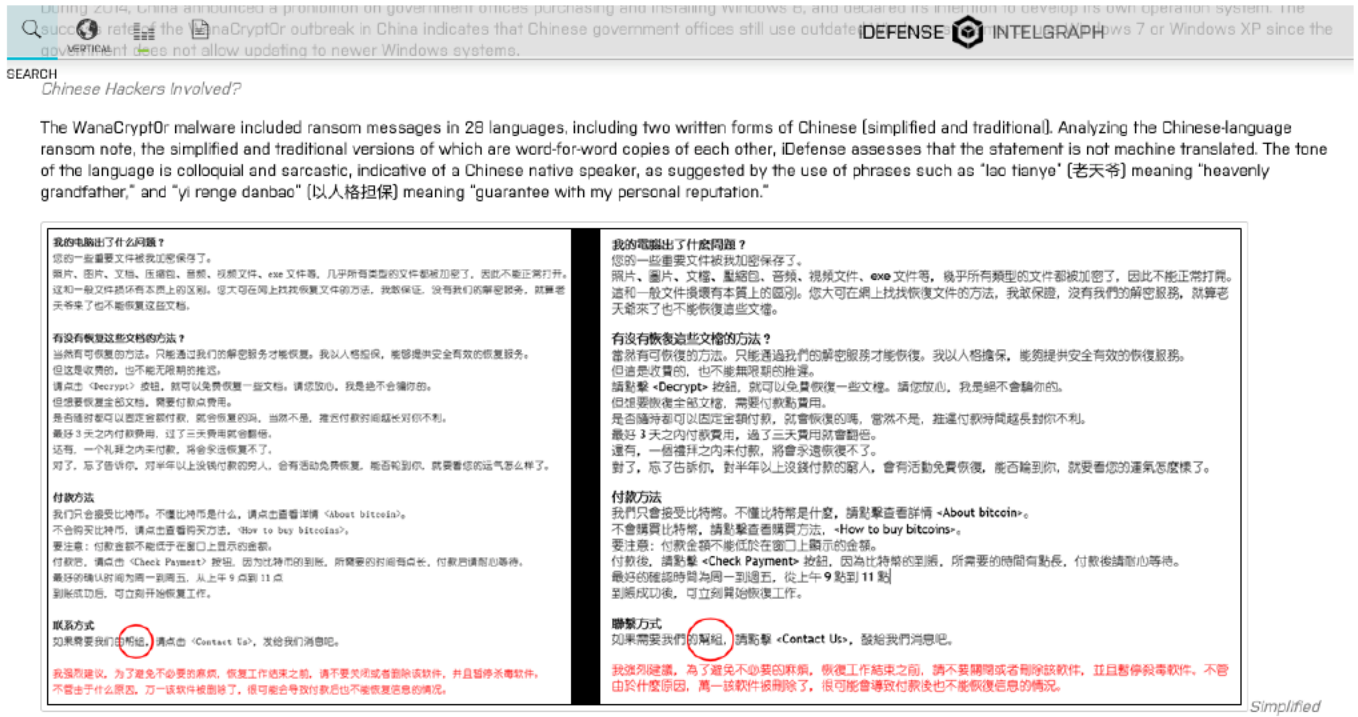
WHO

WHO: Cultural Clues

WannaCry ransomware attack 2017

- **lao tian ye: heavenly grandfather**
- **bangzu or bangzhu : help**

lao tian ye: heavenly grandfather
bangzu / bangzhu: help



Simplified and traditional Chinese ransom messages, showing typographical error

The Chinese ransom statement also contains a typographical error, using "帮组" instead of "帮助" (meaning "to help"). This suggests that the statement was typed using the Chinese Pinyin input method, as the Pinyin representation of 帮组 is *bangzu* and that of 帮助 is *bangzhu*. This error may point to the local origin of the writer: speakers of local dialects in China's northeastern area of Liaoning, Jilin and Heilongjiang provinces often mix up the sounds "z" and "zh." This is enough to create a reasonable suspicion that the actors behind WanaCrypt0r (or at least behind the Chinese language WanaCrypt0r ransom notes) may include native speakers of Chinese, actors familiar with Chinese online jargon, or actors from China's northeastern region bordering North Korea.

Ransom note in Chinese

- **Dialectical clues**
- **Keyboard input clues**

RSAConference2020 APJ

A Virtual Learning Experience

WHY

Why Threat Actors Do What They Do

Credit: Wikimedia Commons.

"War is a continuation of politics by other means" **– Carl von Klausewitz**

Cyberthreat operations are a continuation of politics by other means

- Nation state actors: strategic interests
- Cybercriminals: political system provides constraints and incentives

SANDFISH (Sandworm) Attack Against the Republic of Georgia

- October 28, 2019: thousands of websites crashed or were defaced in Georgia
  - Tension over Georgia's relationship with the United States and NATO
- February 20, 2020: UK and US attribute attacks against Georgia to SANDFISH
  - March 29, 2020: Threat actors uploaded entire Georgia voter database in a Russian-language forum

RSAConference2020 APJ

A Virtual Learning Experience

WHEN

WHEN: Geopolitical Events Could Engender Disruptive and Exploitative Cyberthreat Activity

Date	Event	Past activity
November 21–22, 2020	**G20 Summit meetings**	G20 Summit meetings are popular targets for hacktivist campaigns, including those that conduct denial-of-service attacks, and have also attracted the use of regionally specific techniques, such as the exploitation of vulnerabilities in Korean-language Hangul word processor tools. Threat groups have also used the G20 summit as a lure for phishing campaigns targeting organizations unrelated to the meeting.[50]
September 15–30, 2020	**UN General Assembly 75th Session**	The UN is a frequent hacktivist and cyberespionage target, especially when hosting large member events such as General Assembly gatherings.[51]
Unscheduled	**Global defense and security conferences**	Global military conferences in general are likely to be preferred targets of state-sponsored cyberespionage activity. Accenture iDefense expects SNAKEMACKEREL in particular to target attendees of defense and security conferences in 2020 such as the Underwater Defence & Security Conference, using malicious document attachments and possibly other means.[52]
Unscheduled	**NATO and EU enlargement plans**	In 2017, SNAKEMACKEREL targeted Montenegro government officials prior to Montenegro's accession to NATO. In December 2018, the same group targeted North Macedonian officials during that country's NATO admission. North Macedonia's NATO accession is expected to become official in 2020.[53] Other countries aspiring to join or discussing NATO membership include Bosnia and Herzegovina, Georgia, Ukraine, Sweden and Finland. Countries aspiring to join the European Union include Serbia, Montenegro and Turkey.
Unscheduled	**Sanctions declarations**	Threat groups such as SNAKEMACKEREL, Syrian Electronic Army and Endless Mayfly have responded to sanctions declarations with campaigns of disinformation and access attempts against selected government targets.[54]

Source: Accenture Security 2019 Cyber Threatscape Report

RSAConference2020 APJ

A Virtual Learning Experience

WHERE

WHERE: Navigating a Risky World

- Acquisitions, joint ventures, overseas branches
- Areas of risk
- Country threat landscape

WHERE: Brazil – an Example

- Cybercrime environment
- Human fallibility
- Importance of employee security awareness

RSAConference2020 APJ
A Virtual Learning Experience

What Geopolitical Intelligence May Include

Start with Intelligence Requirements

“The identification, prioritization, and refinement of uncertainties concerning the threat and the battlefield environment that a command must resolve to accomplish its mission.”

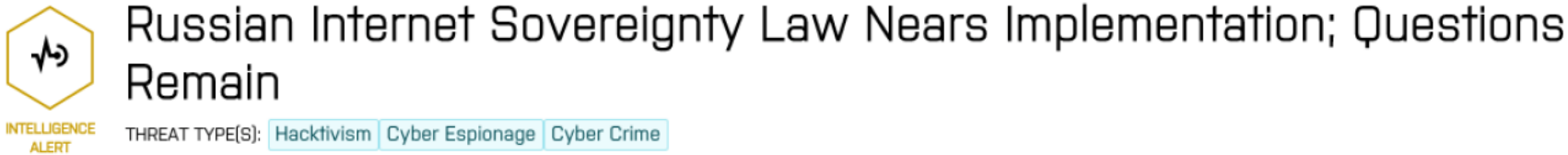
- Collection Management and Synchronization Planning (US Army Field Manual, FM 34-2)

Collection - Analysis - Dissemination

- Intelligence Alert / Report
- Threat Assessment
- Tailored Threat Briefing
- Malicious Event
- Threat Group
- Threat Actor
- Global Events

Report Examples

- Intelligence Alert / Report

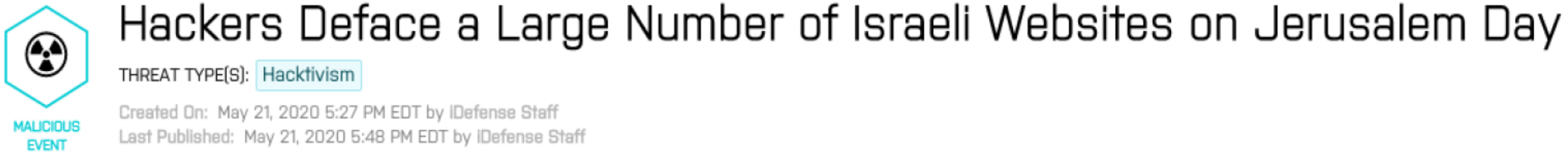


- Threat Assessment

Source: iDefense Intelgraph Research.

Report Examples

- Malicious Event



- Global Event

Source: iDefense Intelgraph Research.

RSAConference2020 APJ
A Virtual Learning Experience

How to Practice Geopolitical Intelligence

Four Key Elements

- Importance of a dedicated team of analysts
  - Hire culturally and linguistically knowledgeable analysts
  - Coordinate with key business units and organization leadership
- Importance of analytic rigor
  - Educate on analytic techniques and discipline
  - Understand your own cognitive biases
- Importance of sources
  - Evaluate sources
  - Do not ignore unreliable sources
- Importance of coordination and communication
  - Develop relationship with key cyber threat intelligence consumers
  - Solicit feedback and incorporate it into future reporting

Helpful Sources

- Structured Analytic Techniques For Intelligence Analysis
  Randolph H. Pherson and Richards J. Heuer Jr.
- Psychology of Intelligence Analysis
  Richard J. Heuer https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf
- Joint Operations (Joint Publication 3-0)
  https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910
- The Diamond Model of Intrusion Analysis
  https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
- Cyber Kill Chain
  https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf
- MITRE ATT&CK; PRE-ATT&CK; and ICS-ATT&CK
  https://attack.mitre.org/
- Listservs: e.g., Sinocism, ASPI Cyber Policy Daily Cyber Digest

Apply What You Have Learned Today

- Next week you should:
  - Familiarize yourself with source materials
  - Set up daily news alerts related to your industry and supply chains
- In the first three months following this presentation you should:
  - Establish an intelligence collection requirements process
  - Analyze relevant past threat activities and define “who” and “why”
  - Analyze threat implications of geopolitical events from daily news alerts
- Within six months you should:
  - Set up a dedicated team to conduct geopolitical intelligence analysis and reporting according to relevant intelligence collection requirements
  - Establish a routine geopolitical intelligence and cyberthreat reporting and briefing to inform decision-makers at the strategic, operational and tactical levels

LEGAL NOTICE & DISCLAIMER

Accenture Security

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects helps organizations' protect their valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

RSAConference2020 APJ

A Virtual Learning Experience

THANK YOU