The Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar

AGENDA

- Team Introductions
- Topic Summary
- Key Findings
- The Grand Cyber Arms Bazaar
- Forecasts
- Impact to Government and Private Sector
- Analytic Deliverable Dissemination Plan
- Q&A

TEAM MEMBERS

Member	Organization
Aaron Henry	FireEye
Clare Boyle	US Government
Guillermo Christensen	Ice Miller LLP
Kyle H.	US Government
Megan Foster	FS-ISAC
Munish P.	US Government
Pipps Nash	
Tony Porter	FON Advisors
Dana M.	***US Government***
Suzel S.	***US Government***

TOPIC SUMMARY

TOPIC DESCRIPTION

The proliferation and commodification of cyber offensive capabilities, through emergence of a "***grand cyber arms bazaar***," is reshaping the cyber balance of power, enabling an expanded array of actors to use cyber for geopolitical impact or economic gain.

This research proposes a framework to distinguish among a growing range of actors and explore the current dearth of deterrence, lack of redlines, and inherent unintended consequences of cyber engagement.

RESEARCH QUESTIONS

- How will the proliferation of cyber capabilities change the cyber threat landscape?
- How can executives prioritize concern among an expanding array of threat actors who have access to sophisticated technical capabilities?
- What policy challenges arise from cyber proliferation?
- What are some alternative outcomes for the trends we have identified?

KEY FINDINGS

- The proliferation and commodification of cyber capabilities is enabling an expanding array of state and non-state actors to use cyber means for geopolitical impact or economic gain.
- Foreign actors will achieve varying levels of success in using cyber means for profit, collection, and attack. We distinguish actors as established, emerging, or opportunistic based on the organizational maturity of their cyber programs. One wildcard is the ability of actors to quickly buy, build, or bridge sophisticated cyber capabilities and processes.
- Policy challenges related to deterrence, redlines, and escalation have resulted from the lack of cyber norms and challenges faced by the West in imposing consequences for malicious cyber activity, including actions that fall below the threshold of war. This could drive rapid escalation in international crises unless we arrive at an inflection point that drives collective action to contain the cyber drivers of geopolitical instability.
- Private and public sector executives will need to posture their organizations for an increasing risk of surprise in cyber space. They will increasingly need to account for geopolitical developments in their cyber defenses and find ways to bolster operational and technical resilience. New approaches for public/private collaboration will be required as private sector firms increasingly become “front line” targets for foreign actors seeking to shape Western policy using tactics short of war.

CYBER THREAT LANDSCAPE

More Actors, Capabilities and Connectivity

- **Actors** – An expanding array of state and non-state actors with access to various cyber tools or weapons, which may be employed for collection, financial gain, surveillance, or attack.

- **Capabilities** – A low entry barrier for new actors because cyber tools and expertise are hard to contain or control.

- **Connectivity** – Growing connectivity opens a larger attack surface and expands the reach of a growing set of adversaries. In some cases, connectivity may lead to "collateral damage" if a cyber weapon propagates beyond its intended target(s).

APPROACHES TO ACQUIRING CYBER CAPABILITY

Buy, Bridge, Build

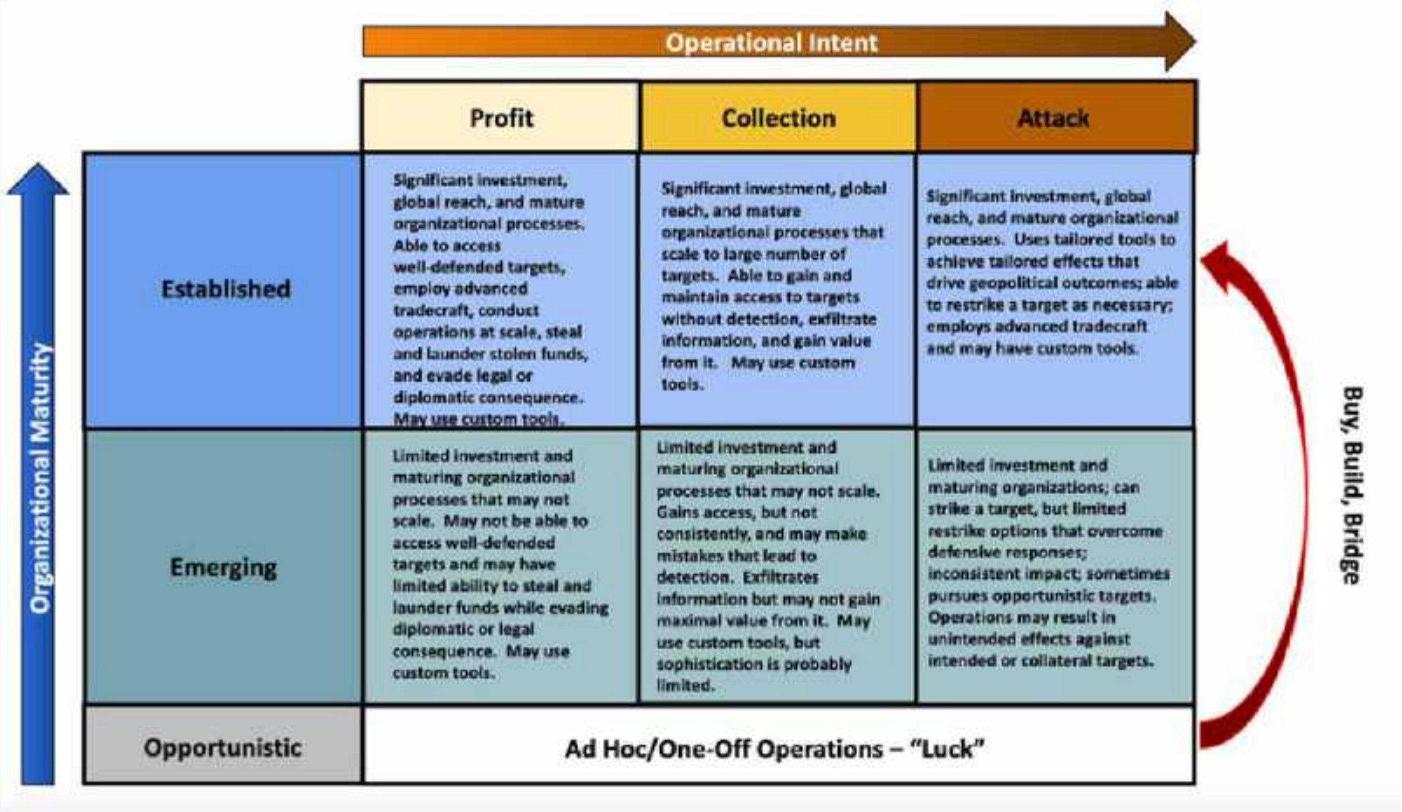
- **Buy –** Actors can purchase capabilities of varying complexity and effectiveness from commercial sources or the dark web.

- **Bridge –** Forge partnerships with commercial firms or cyber criminals to acquire capabilities and the organizational processes to employ them as a temporary measure until indigenous capabilities are mature.

- **Build –** One expert opined that nations seeking to incorporate cyber attack into their military capabilities would eventually seek indigenous capabilities, rather than relying on external sources.

THE GRAND CYBER ARMS BAZAAR

A Framework for Categorizing Sophistication



Operational Intent

Organizational Maturity

Buy, Build, Bridge

	Profit	Collection	Attack
Established	Significant investment, global reach, and mature organizational processes. Able to access well-defended targets, employ advanced tradecraft, conduct operations at scale, steal and launder stolen funds, and evade legal or diplomatic consequence. May use custom tools.	Significant investment, global reach, and mature organizational processes that scale to large number of targets. Able to gain and maintain access to targets without detection, exfiltrate information, and gain value from it. May use custom tools.	Significant investment, global reach, and mature organizational processes. Uses tailored tools to achieve tailored effects that drive geopolitical outcomes; able to restrike a target as necessary; employs advanced tradecraft and may have custom tools.
Emerging	Limited investment and maturing organizational processes that may not scale. May not be able to access well-defended targets and may have limited ability to steal and launder funds while evading diplomatic or legal consequence. May use custom tools.	Limited investment and maturing organizational processes that may not scale. Gains access, but not consistently, and may make mistakes that lead to detection. Exfiltrates information but may not gain maximal value from it. May use custom tools, but sophistication is probably limited.	Limited investment and maturing organizations; can strike a target, but limited restrike options that overcome defensive responses; inconsistent impact; sometimes pursues opportunistic targets. Operations may result in unintended effects against intended or collateral targets.
Opportunistic	Ad Hoc/One-Off Operations – "Luck"		

POLICY CHALLENGES

Deterrence, Redlines, and Escalation

- **Deterrence** - Non-state actors represent a unique challenge to deterrence because they are often not susceptible to diplomatic or military suasion in the same manner as nation-states.

- **Redlines** - The lack of clear international norms regarding the use of cyber capabilities has led to the creation of unwritten rules among cyber actors on how to operate.

- **Escalation** - As cyber effects move increasingly closer to what are universally viewed as acts of war, there is the increasing potential to cross a redline that elicits kinetic or military response.

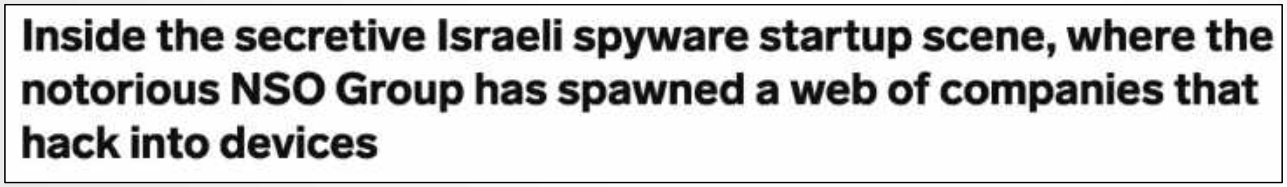
FORECASTS: A FEW FUTURES TO CONSIDER

- **Rapid Escalation**
  - ***Assumptions:*** cyber proliferation continues; lack of cyber norms; foreign actors take increasingly risky actions with little fear of repercussion; attribution remains hard.
  - ***Scenario:*** High-visibility/impact cyber attack during elevated tensions between two regional rivals; sponsor of the attack is unclear; tensions further inflamed, making de-escalation more difficult.
- **Inflection Point**
  - ***Assumptions:*** Cyber norms exist; mature communication channels have been established for dealing with fast-breaking cyber crises.
  - ***Scenario:*** High-visibility/impact cyber attack during elevated tensions; cyber norms identify a standard of attribution before responding; pre-established communication channels quickly establish third-party responsibility for the cyber attack, preventing further escalation.

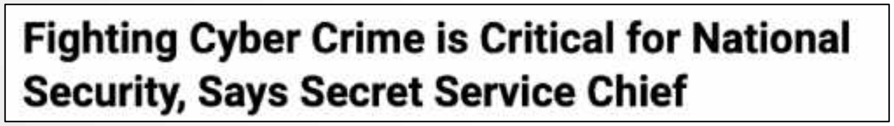
IMPACTS TO GOVERNMENT AND PRIVATE SECTOR

- Executives in both sectors must posture their organizations for a growing risk of surprise in cyberspace
- As more actors use cyber effects to advance geopolitical aims, organizations increasingly will need to integrate world events into their network defense processes
- Grappling with an increasing risk of surprise will require proactive efforts to increase the operational and technical resilience of organizations
- Government entities, researchers, and think tanks can likely assist public and private sector organizations in posturing for this new environment
- Senior executives can prepare their workforces for this environment by developing a consistent and multi-dimensional communications strategy used at all management levels
- New approaches for government and private sector collaboration must be created to ensure national security as private sector firms increasingly become "front line" targets for foreign actors seeking to shape Western policy

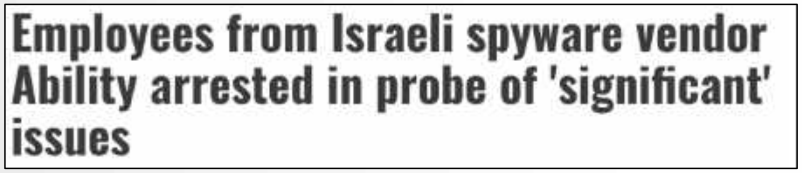
VALIDATION: RECENT HEADLINES



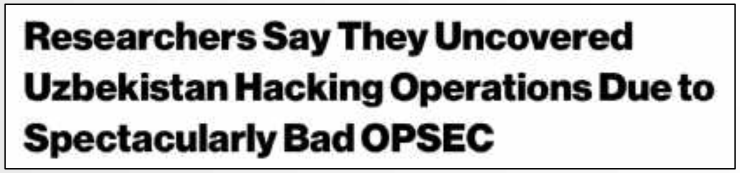
Inside the secretive Israeli spyware startup scene, where the notorious NSO Group has spawned a web of companies that hack into devices



Fighting Cyber Crime is Critical for National Security, Says Secret Service Chief



Employees from Israeli spyware vendor Ability arrested in probe of 'significant' issues



Researchers Say They Uncovered Uzbekistan Hacking Operations Due to Spectacularly Bad OPSEC

DELIVERABLE DISSEMINATION PLAN

Government

- **Congressional Cyber Caucus**
- **Cyberspace Solarium Commission**
- **Strategic Multilayer Assessment (DoD)**

Conferences

- **DC Analysts' Roundtable, Annual***
- Black Hat/Defcon (planned)
- RSA (planned)
- International Association of Privacy Professionals (IAPP) (planned)
- International Conference on Cyber Engagement (ICCE) (planned)

Academia

- West Point, Army Cyber Institute
- Virginia Polytechnic Institute and State University
- Columbia University, School of Int'l and Public Affairs
- New York University, Center for Global Affairs
- Fordham University, Int'l Conference on Cyber Security
- Stanford, Center for International Security and Cooperation

Media & Press

- Reuters
- Cyberscoop
- Motherboard
- Axios

DELIVERABLE DISSEMINATION PLAN

Think Tanks, Industry, and Nonprofits

- **Intelligence & National Security Alliance (INSA)**
- **International Institute for Strategic Studies (IISS)**
- **Financial Systemic Analysis and Resilience Center**
- **Atlantic Council**
- Council on Foreign Relations - Digital and Cyberspace Policy Program
- Aspen Institute Cyber & Technology Program
- MITRE
- Multi-State Information Sharing & Analysis Center (MSISAC)
- InfraGard Chapters (Nation-wide)

completed

Thank you!

Questions and Comments?

TEAM PHOTO

Geopolitical Impact on Cyber Threats from Nation-State Actors