Labyrinth

SECURITY GROUP

A shared sense of purpose

Cyber Targeting Cycle (CTC)

Labyrinth
SECURITY GROUP

Labyrinth Security Group

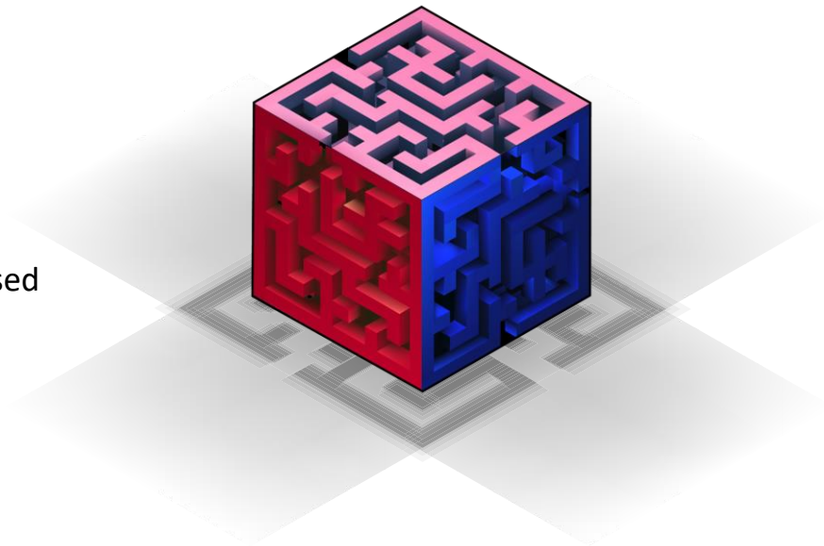
A shared sense of purpose

The Labyrinth Security Group is a consortium of passionate and dedicated cyber security professionals with a desire to contribute to the cyber security community by sharing knowledge and concepts through collaboration.

Sharing Cyber Security Knowledge & Community Collaboration

- Business Enablement
  - Strategy
  - Business Alignment
  - Architecture & Design
- Security Operations
- Risk Management
- Identity Access Management
- Legal & Regulatory
- Governance
- Research and Development
- Cyber Threat Intelligence

Purple Team
Facilitate collaboration toward a common business goal



Red Team
Adversary Emulation & Campaign-based Testing

Blue Team
Defensive and Counter Operations

Labyrinth SECURITY GROUP

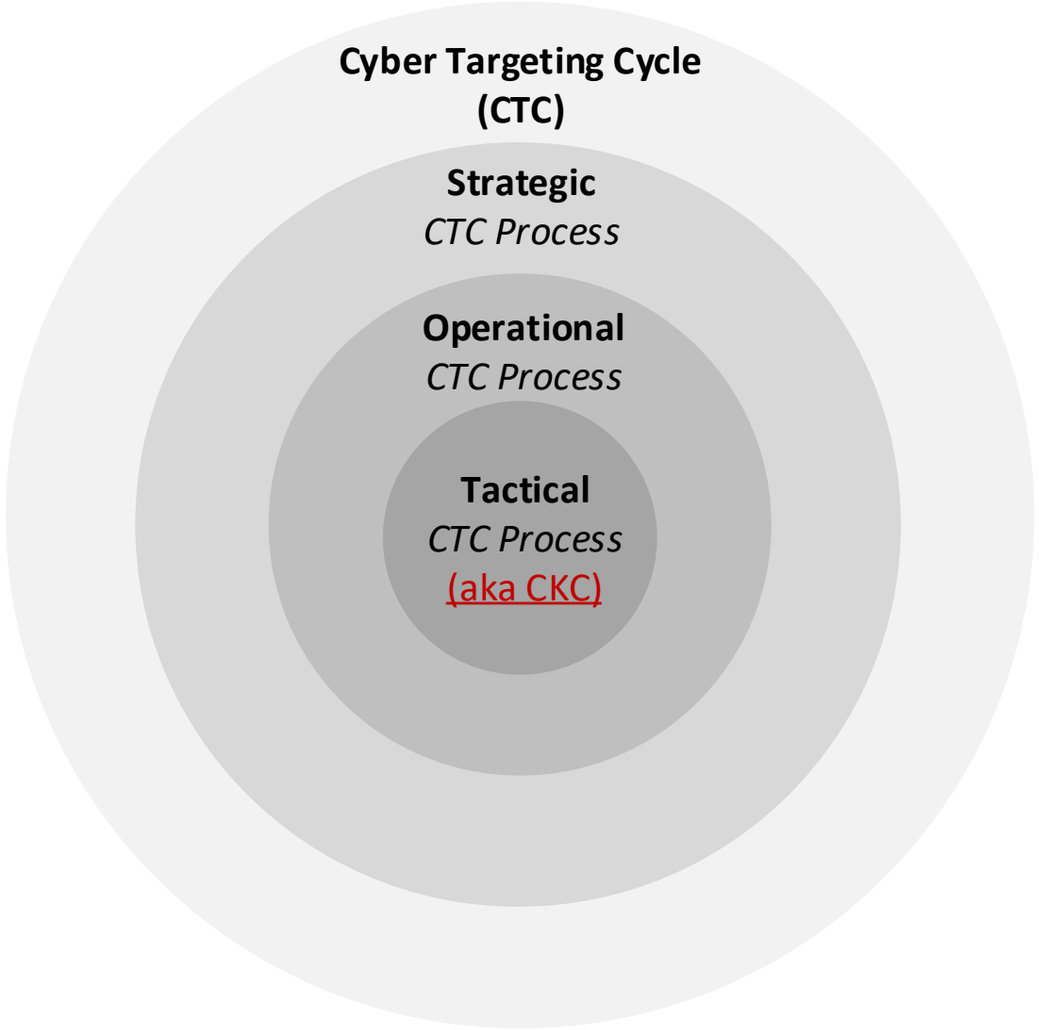
CTC Overview

A shared sense of purpose

The Lockheed Martin Cyber Kill Chain (CKC) is part of a larger cycle – The Cyber Targeting Cycle (CTC)

CTC Slide Deck Overview

- Description of additional levels and steps which lead to cyber attack execution (e.g. rationale, desired end-state, objectives, assessment measurement criteria, planning, target development, etc.)
- Cyber security professionals should have an understanding of potential adversaries and probability in order to develop appropriate defense posture, counter measures and adequately manage risk
  - Private sector organizations are also part of the national critical infrastructure and should adequately defend themselves
- Lets pull the thread on the Cyber Targeting Cycle (CTC) using an "alleged" complex nation-state use case – Operation Olympic Games ("Stuxnet")



[1]The source material used for this presentation was derived from publicly available information
[2]The intent is to use Stuxnet as a use-case to support the Cyber Targeting Cycle discussion

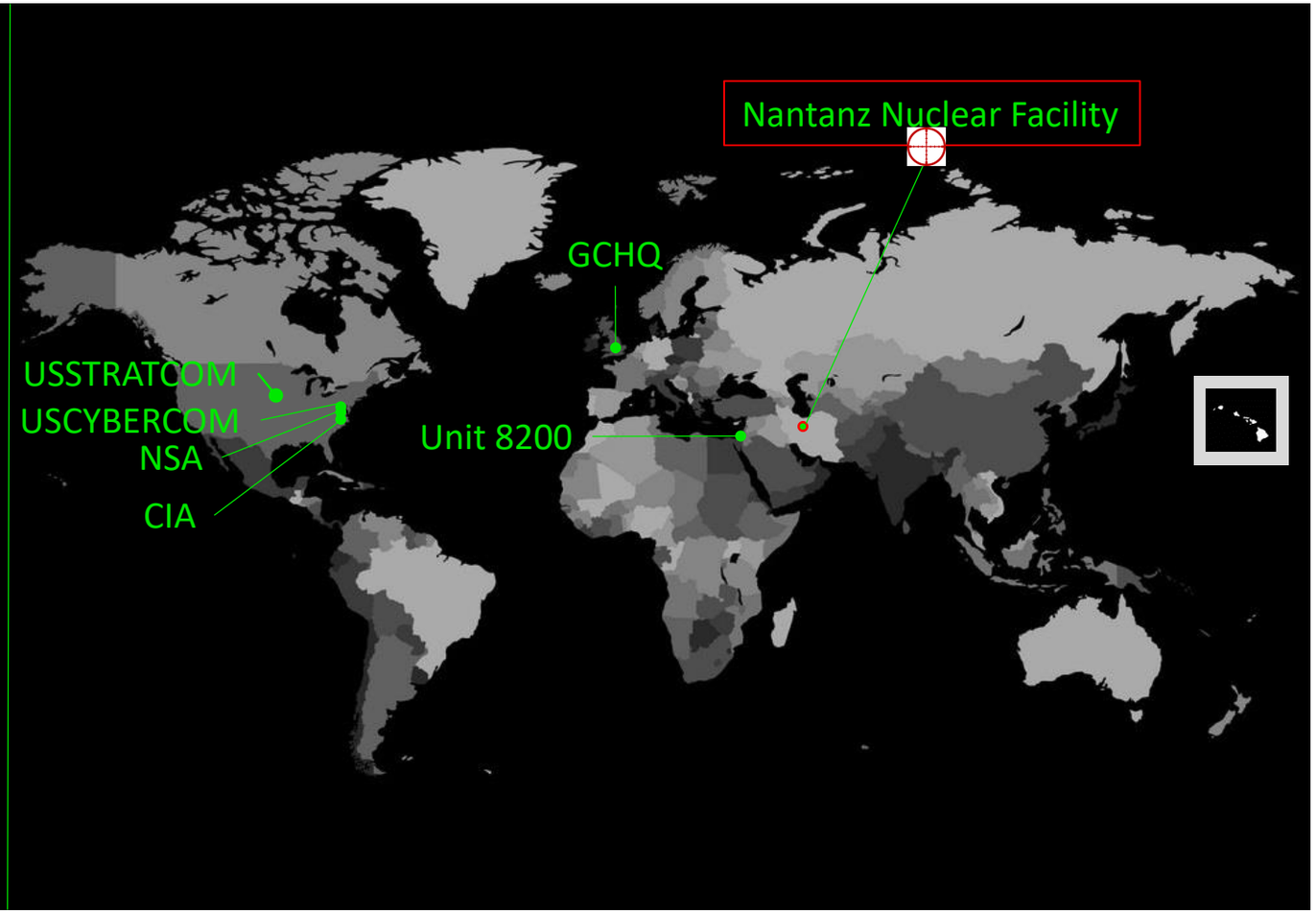
Labyrinth SECURITY GROUP

Use Case: Operation Olympic Games (Stuxnet)

A shared sense of purpose

Characteristics

- Alleged Actors: United States, Great Britain, Israel
- Target(s): Iran Nuclear Development Facility Centrifuge PLCs
- Objective(s):
  - Deny Iran a military nuclear capability
  - Slow down nuclear program-Buy time
  - Covert kinetic "cyber target"
  - Get Iran to negotiating table
- U.S. Cyber Authorities:
  - POTUS approval
  - USSTRATCOM/USCYBERCOM execution
- Cut Off Date: 1/20/2009,
- **Assessment:**
  - Coalition: Failed to meet U.S. objectives
  - Iran: Political isolation, economic sanctions, program development impeded ~1 yr, followed by exponential nuclear development growth



Labyrinth SECURITY GROUP

Campaign Timeline

A shared sense of purpose

Operation: Olympic Games

- 1957 Iran starts a nuclear R&D program
- 1967 U.S. pledges nuclear capability support to Shah of Iran
- 1979 Iranian Revolution – U.S. relations impact
- 1987 Pakistan transfers nuclear tech to post revolution Iran
- 2007 Israel conducts kinetic op against Syrian nuclear facility
- 2007 US Israeli concerns results in non-kinetic COAs against Iran
- 2006-2007 US considers and approves cyber approach to avoid being dragged into a war by Israel
- 2008-2009 Multi-national Inter-agency Ops planning and execution begins
- 2010 Alleged Israeli "Stuxnet" release into the wild
- 2010 Global infection
- 2010 Public Domain discovery – Coined "Stuxnet"
- 2010 U.S. DHS Responds to newly discovered "Stuxnet" cyber threat
- 2010-2011 CyberOp resulted in 1 year slowdown of Iranian nuclear program
- 2011-2012 Continued cyber target development
- 2012 Automated termination embedded in code

Cyber Capabilities: ***Unlimited Range, High Speed, Low Signature, Low Cost***

CTC Discussion

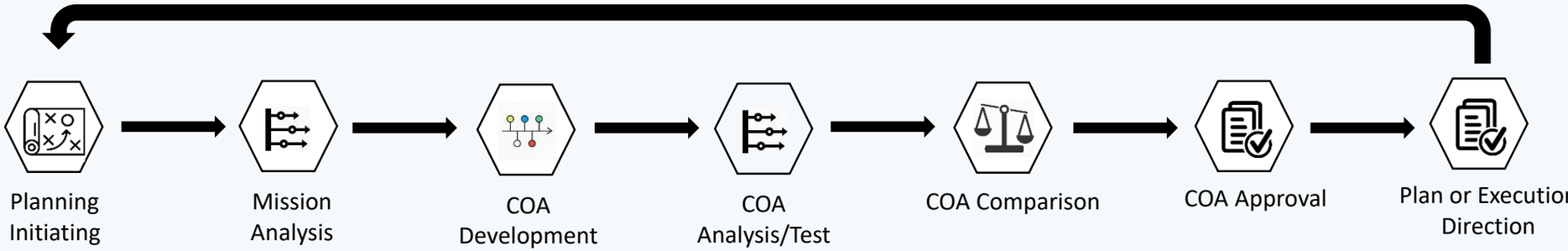
Cyber Targeting Cycle Discussion

- Complex, high stakes, offensive cyber operations require planning and resources
  - There must be a Time Sensitive Target (TST) cycle in place to support small windows of opportunity
- Robust formal/informal CTC is used to inform decision-makers (cyber criminals, hactivists, military, nation-state, etc.)
- In this discussion, I suggest the Lockheed Martin Cyber Kill Chain is the tactical level of the CTC

Labyrinth SECURITY GROUP

CTC Strategic Level

A shared sense of purpose



Planning begins with authoritative approval	Analyze and restate strategic objective for approval and subordinate planning	**Course of Action (COA)** provides options to meet objective end-state for decision makers consideration	Conduct COA Pro/Con analysis	Independent COA review and identification of option with highest success potential	Estimates and recommended COA presented for authoritative approval	Concept of Operation (CONOP) clearly and concisely expresses operational intent and actions

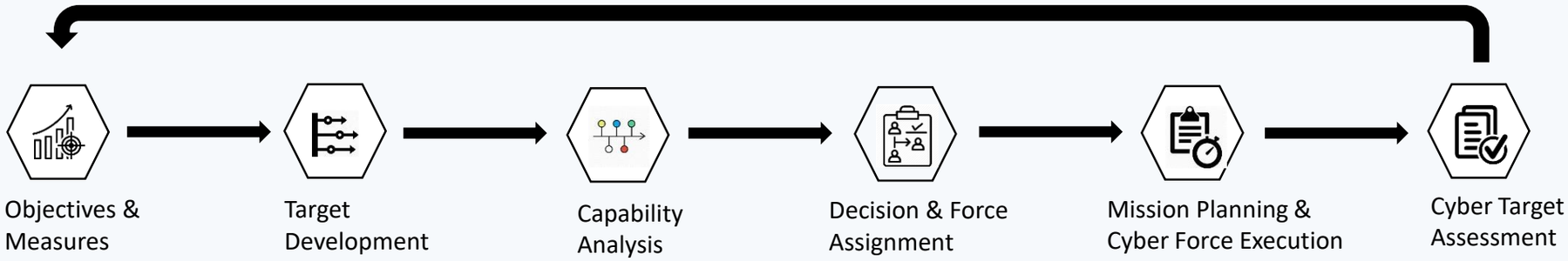
Determine cybersecurity objectives, guidance and required resources to achieve objectives and desired end-states

"The ability to act at scale and speed" - Modernized, Modular, Agile, Flexible, Scalable, Orchestrated

Labyrinth SECURITY GROUP

CTC Operational Level

A shared sense of purpose



Cyber end state, objectives and success measures	Cyber target development & prioritization	Cyber capability analysis	Operational authority decision and cyber force assignment	Mission planning and cyber force execution	Cyber target assessment

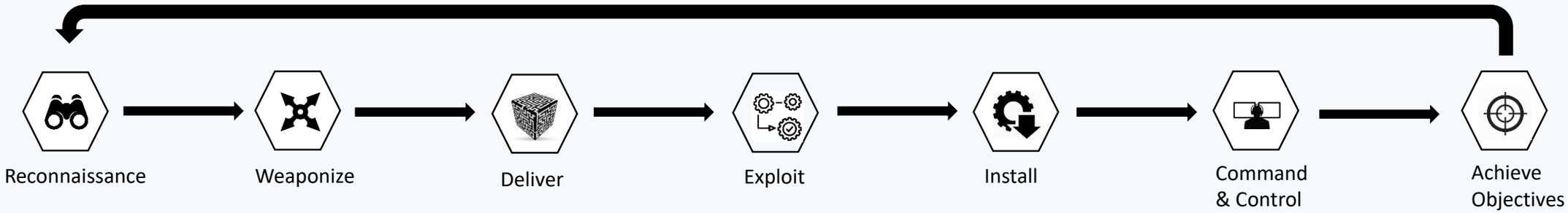
Operations are designed, planned, conducted, sustained, assessed, and adapted to accomplish strategic goals within acceptable scope

"The ability to act at scale and speed" - Modernized, Modular, Agile, Flexible, Scalable, Orchestrated

Labyrinth SECURITY GROUP

CTC Tactical Level

A shared sense of purpose



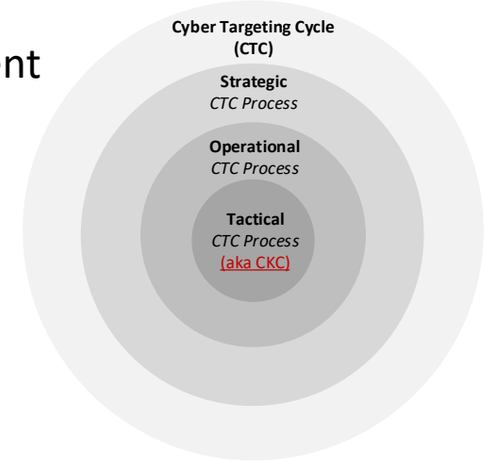
Reconnaissance	Weaponize	Deliver	Exploit	Install	Command & Control	Achieve Objectives
Harvesting email addresses, conference information, etc.	Coupling exploit with backdoor into deliverable payload	Delivering weaponized bundle to victim via email, Mobile Code, USB, Supply Chain, etc.	Exploiting a vulnerability to execute code on victim's system	Installing malware on the asset	Command channel for remote manipulation of victim	With "hands on keyboard" access, intruders accomplish their original goals

Tactical application of cyber force action in accordance with plan to meet operational and/or strategic effects

"The ability to act at scale and speed" - Modernized, Modular, Agile, Flexible, Scalable, Orchestrated

Conclusion

- The cyber kill chain is the tactical sub-process of a broader process - the Cyber Targeting Cycle
  - Cyber attacks require a network of organized actors to plan, coordinate, execute/monitor, and assess the operations effectiveness – It is not fire and forget
  - There are many linkages between cybersecurity and intelligence disciplines
    - Target, Human, Counter-Intel, Open Source, Signal, Geospatial, Fusion, All-Source
    - Identifying the target network is a cyber intelligence target development function
    - Creating predictive capabilities will require intelligence tradecraft/methodologies and AI/ML
    - Cyber Threat Modeling and Simulation, third party intelligence reports, publicly available information, combined with internally developed reports can help with cybersecurity design and planning (*Develop and test your plans!*)
      - Verizon 2019 Data Breach Investigations Report (pdf)
      - DHS Cybersecurity Risk Determination Report May 2018 (pdf)
  - Most enterprise organizations need to modernize and redesign security architecture based on current advanced persistent threats - Consider zero trust architecture, defensible architecture, or a hybrid architecture
    - Zero Trust is a paradigm shift but you will be surprised what you can do to with existing technology platform mechanisms to potentially improving security posture, without capital expenditures – Check out the SANS webcast below for ideas
      - SANS Zero Trust Architecture Webcast (by Justin Henderson)
      - https://www.youtube.com/watch?v=5sFOdpMLXQg&t=1792s



Sources

- Joint Pub 5-0 Joint Planning (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf)
- Joint Pub 3-12 Cyber Operations (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf)
- Joint Pub 3-60 Joint Targeting (https://www.justsecurity.org/wp-content/uploads/2015/06/Joint_Chiefs-Joint_Targeting_20130131.pdf)
- Levels of War (https://www.doctrine.af.mil/Portals/61/documents/Volume_1/V1-D34-Levels-of-War.pdf)
- Zer0Day (2016) (https://www.youtube.com/watch?v=oz585G-6NBA)
- How a Secret Cyberwar Works (https://archive.nytimes.com/www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-programworked.html)
- Iran's Nuclear Program Timeline and History (https://www.nti.org/learn/countries/iran/nuclear/)
- Israeli Test on Worm Called Crucial in Iran Nuclear Delay (https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html)