Assessing Actions Along the Spectrum of Cyberspace Operations

Presented by USCYBERCOM/JA

This presentation does not necessarily reflect the position of the US Government.

Spectrum of Cyber Operations

Access Operations
• Digital intelligence
(e.g., stealthy implant)

Cyber Disruption
•Interrupt the flow of information or function of information systems

Change, delete, manipulate data,
(e.g., changing a word in a document);
Modify software to cause system glitches,
(e.g., causing a reboot or causing a file to close);
Disrupting communications, or command and control
(e.g. blocking emails, web forums, telephone communication)

Cyber Attack
• Use of force
• Physical damage or destruction
• Physical injury or death

Very stealthy — Less stealthy

Spectrum of Cyber Operations

With that background, we will discuss several real world and exercise examples of cyber operations to determine where they fall on the spectrum of cyber operations

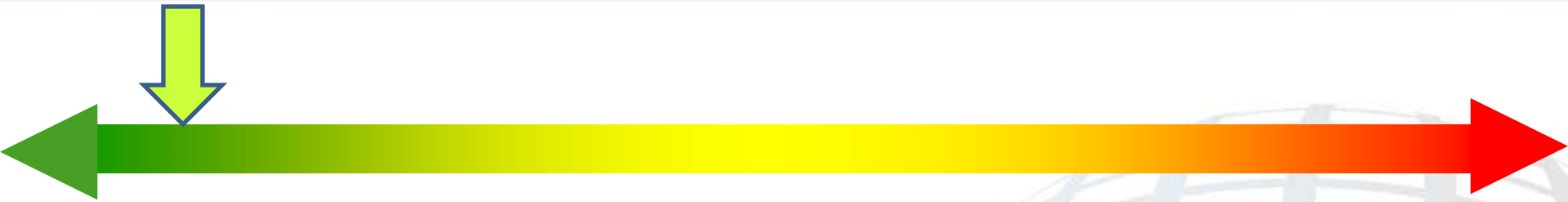
Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
•Interrupt the flow of information or function of information systems without physical damage or injury

Cyber Attack
• Use of force
• Physical damage or destruction
• Physical injury or death

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

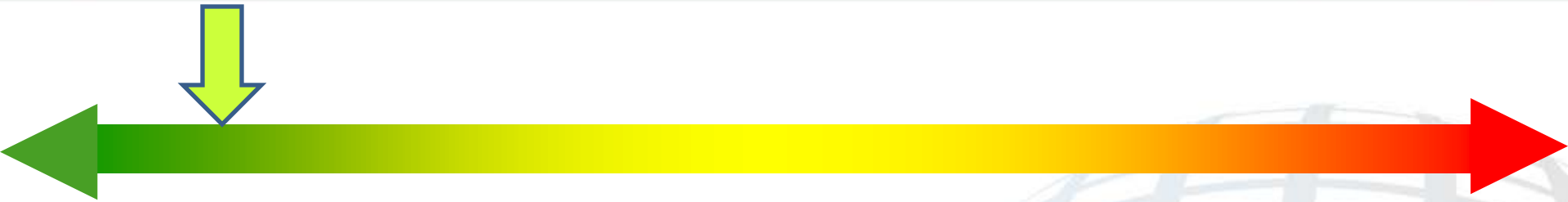
Cyber Attack
• Physical damage to property or injury to persons

Operation Buckshot Yankee Implant

- Code embedded in flash drive
- Downloaded when inserted into computer
- (Ran code to enable exfiltration)

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

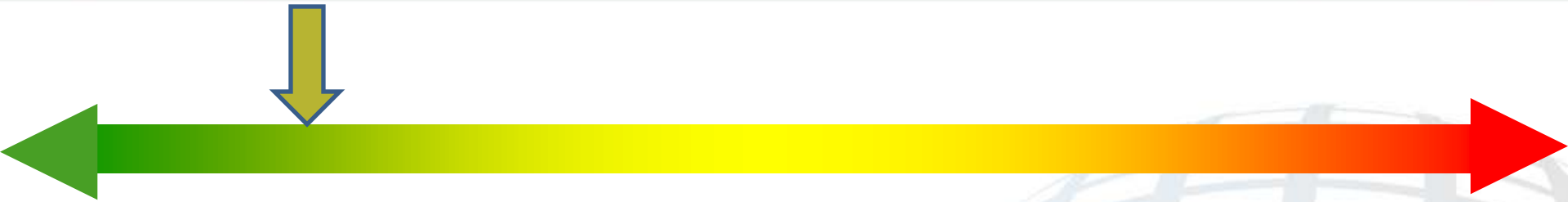
Cyber Attack
• Physical damage to property or injury to persons

Change Data with No Physical Damage to Gain Access

- Erase admin logs
- Cause reboot to upload or activate program
- Install program

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

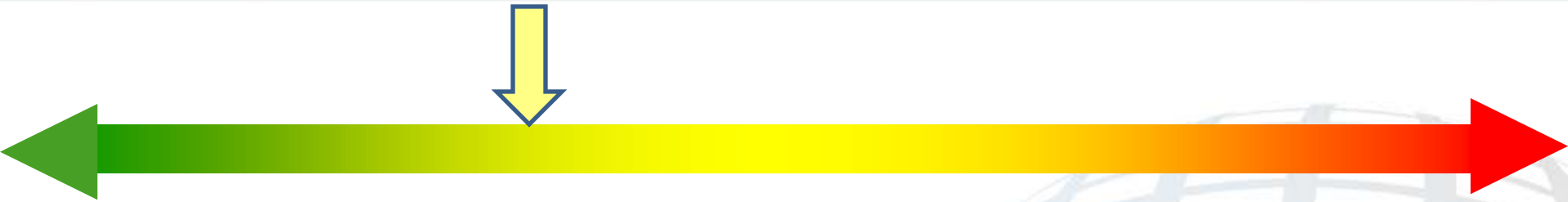
Cyber Attack
• Physical damage to property or injury to persons

Cyber Shock Wave—Move One

- Malware downloaded to cell phones during basketball game
- Designed to spread to linked computers
- Botnet ready to order

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

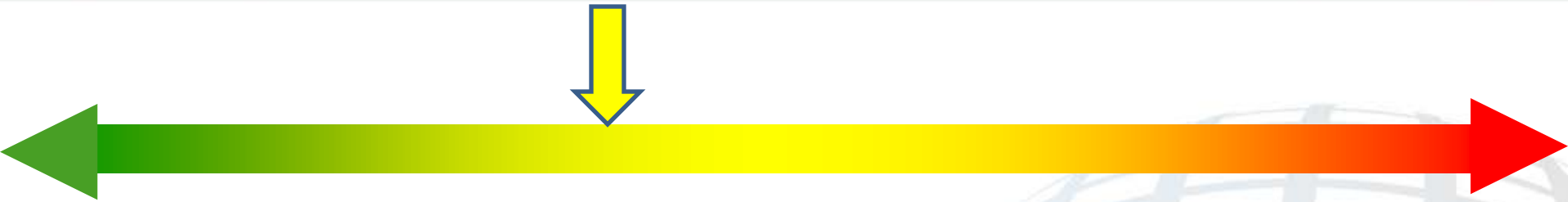
Cyber Attack
• Physical damage to property or injury to persons

Small scale Denial of Service against Non-Government Adversary

- Block adversary publication of a magazine or pamphlets (e.g. Inspire)
- Block email communications
- Block access to website

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

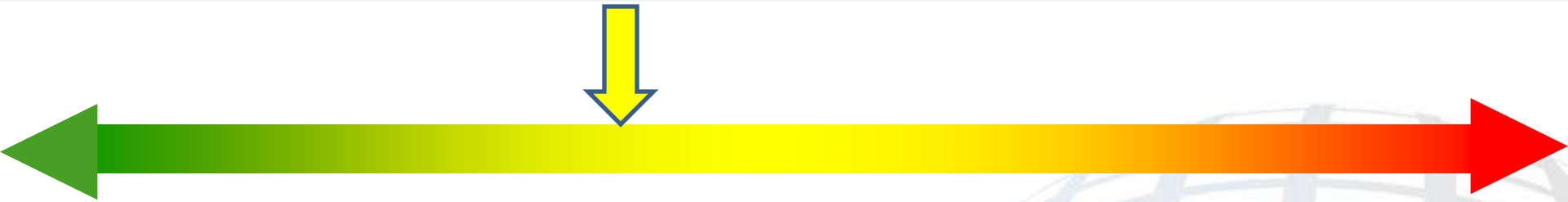
Cyber Attack
• Physical damage to property or injury to persons

Delete or Change Data of Non-Governmental Adversary (with no physical damage or injury to persons)

- Delete web documents or files from computer
- Change information in articles or propaganda
- Manipulate information to render instructions ineffective
- Change location of tactical rendezvous

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

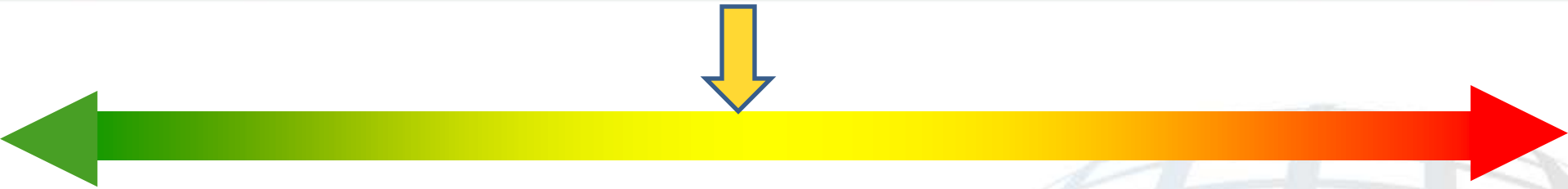
Cyber Attack
• Physical damage to property or injury to persons

Operation Aurora

- Access to systems of Google and more than 20 other companies, including web security, defense industry
- Google attributed to China Politburo officials and assisting organizations
- Actions lasted several months
- Data stolen
- Security codes modified

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

Cyber Attack
• Physical damage to property or injury to persons

U.S. and South Korea 2009

- 27 Government and commercial sites hit with a denial of service
- Estimated over 50K+ computers in botnet sending requests
- Targeted NY Stock Exchange, NASDAQ, Yahoo financial, Dept of Transportation, Treasury, FTC, White House, Secret Service
- DDOS lasted from hours to a few days

Very stealthy — Less stealthy

Spectrum of Cyber Operations

Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

Cyber Attack
• Physical damage to property or injury to persons

Estonia 2007

- Intermittent DDOS against government and businesses over the course of a month
- Botnets used; actions transited over 170 countries
- Online banking down for most of the month
- Government unable to send emails for days at a time
- Data changed on websites including defacement and propaganda
- Primarily economic impact and degraded communications

Very stealthy — Less stealthy

Spectrum of Cyber Operations

Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems

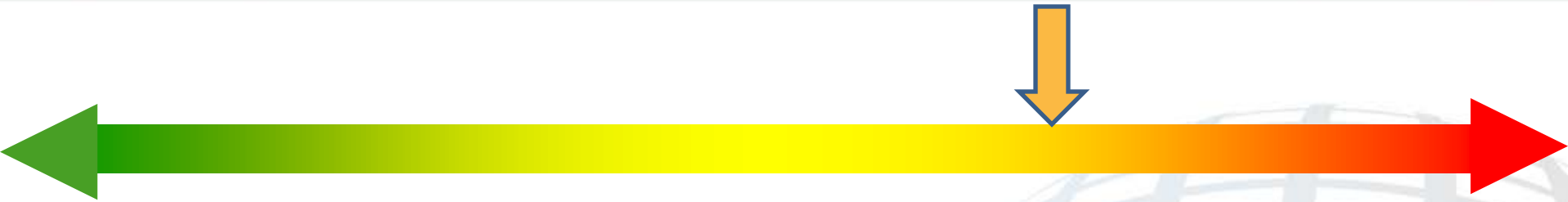
Cyber Attack
• Physical damage to property or injury to persons

Estonia 2007

- NOTE: Estonia and NATO stated these actions did not constitute a use of force
- We may consider actions less than Estonia as less than a use of force
- Many cyber disruption actions fall below this threshold
  - (Month long DDOS against banking, government web-sites, communication)

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
•Interrupt the flow of information or function of information systems

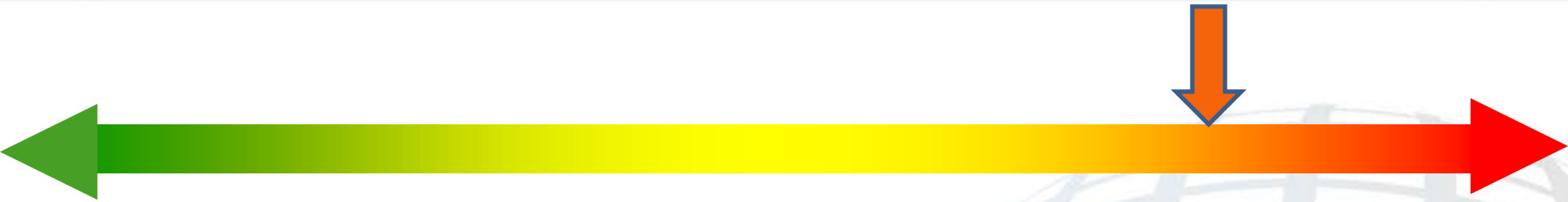
Cyber Attack
• Physical damage to property or injury to persons

Cyber Shock Wave—Move 2

- Botnet spread through malware-generated emails
- Civilian SCADA outage with no physical damage
- 40 Million lost electricity in Eastern U.S. for hours to days
- 60 Million lost cell phone access for days
- Wall Street down for 1 week

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
•Interrupt the flow of information or function of information systems

Cyber Attack
• Physical damage to property or injury to persons

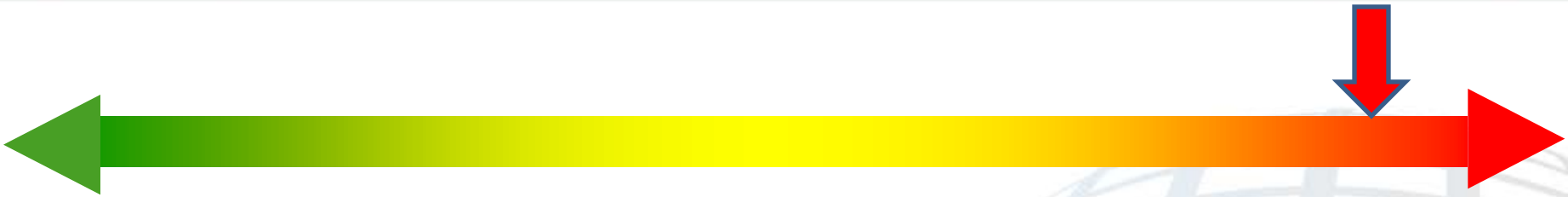
Cyber Storm

- SCADA outage with no physical damage
- Affects Government and critical infrastructure
- Air Traffic Control lost for limited period
- Loss of government communications for days
- D.C. Metro shut down for days

Gray area: may be viewed as attack depending on severity

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
•Interrupt the flow of information or function of information systems

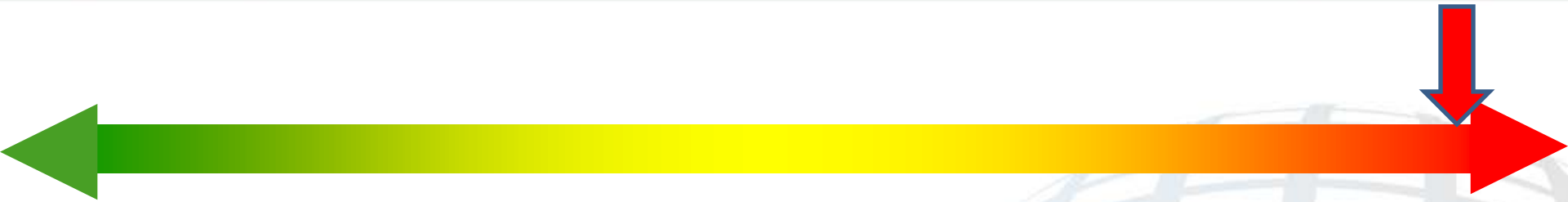
Cyber Attack
• Physical damage to property or injury to persons

Stuxnet

- Precision-Effect Code infiltrated Iran's nuclear facilities for uranium enrichment
- Cyber code altered rotation speed of centrifuges
- Over 1000 centrifuges damaged

Very stealthy — Less stealthy

Spectrum of Cyber Operations



Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
•Interrupt the flow of information or function of information systems

Cyber Attack
• Physical damage to property or injury to persons

Deleting or Manipulating Data
(causing physical damage and injury)

- Alter subway data to cause trains to collide
- Altering flight paths causing planes to collide
- Altering or deleting information in medical and pharmaceutical records causing serious illness and death when patients treated

Very stealthy — Less stealthy

Spectrum of Cyber Operations

Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
•Interrupt the flow of information or function of information systems

Cyber Attack
• Physical damage to property or injury to persons

Cyber Attack During Conflict

- Damage command and control systems
- Cause in-flight failure on military aircraft
- Cause detonation at military fuel depot

Very stealthy — Less stealthy

Spectrum of Cyber Operations

Ping, Map or Probe	Buckshot Yankee •Erase logs •Install code	CSW Move One •Implant malware •Create botnet	Degrade Service or access to info	Delete or change adversary data with no phys. damage or injury China & Google	US/ROK •DDOS with minor impact	Estonia • Govt & Banking down for most of a month	Cyber Shock Wave •SCADA outage with no physical damage • Primarily private systems	Cyber Storm •SCADA outage with no physical damage • Effected Govt & critical systems	Change Data • Causes injury or damage	Stuxnet •Damage 1000 centri-fuges Attack in conflict • Destroy C2, fuel, planes, ships

Access Operations
• Digital intelligence (e.g., stealthy implant)

Cyber Disruption
• Interrupt the flow of information or function of information systems without physical damage or injury

Cyber Attack
• Physical damage to property or injury to persons

Very stealthy — Less stealthy