Cyber Fratricide

Dr. Samuel Liles
Purdue CyberForensics Laboratory
Purdue University
Jacob Kambic
Purdue CyberForensics Laboratory
Purdue University

Why this research?

In 2011 I was asked how to de-conflict the missions of the J2, J3, J6 and I wondered what in the world the requester meant.

The scenario at that time was, “What if the 2 did something that got the 6 in trouble, or had an asset or capability that exposed the 3 to harm or risk?” My answer at the time was, “Who’s on first?” There has been some doctrinal changes since then but the question remains an open one. What does cyber fratricide look like and how will you fix it?

Introduction

- Continental staff system
  - Intelligence officer is identified by the number 2
  - Operations officer by 3
  - Communications officer by the number 6
- Cyber Fratricide
  - The unintentional impedance or interference between operational/tactical elements of friendly forces in the cyber realm, and can involve compromise or liquidation of assets, information, or capabilities.

Points of discussion

- When discussing any conflict domain, assets are conventionally color-coded,
  - Red indicating enemy assets
  - Green indicating all or neutral assets
  - Blue indicating friendly assets.
  - Blue can be further separated into intelligence, operational, and domestic assets.
- Three forms of cyber fratricide.
  - Blue operational entity on blue intelligence entity because these two entities are specifically not in close, bidirectional communication.
  - Blue operational entity on green due to close association with a red information asset.
  - A third form of cyber fratricide occurs due to ineffectual use of the area of operation paradigm and involves blue military operations acting on blue domestic assets in contravention of national laws and norms,

Blue on Blue

- Communications officers may be called upon to execute/conduct offensive activities (Computer Network Attack) that transit a “blue” network.
- Such a situation involves the first form of cyber fratricide— it is possible for any munitions, regardless of domain, to injure friendly troops (or capability) thus creating blue on blue fratricide?
- Blue network could include private or industry telecommunications infrastructures

Issue 1

- What about blue operational entity on blue intelligence entity?
  - Valid concern
  - Kinetic v. Cyber is an issue (blowing up data center)
  - Cyber v. Kinetic is an issue (integrity of weapons targeting data)
  - Growing issue

Blue on Green

- Consider Green information asset housed in Red data center or using red information infrastructure.
- Area of operations construct issues
  - Information asset may be accessed and leveraged by a terrorist cell in Afghanistan that is proxied through Russia by way of a Chinese Internet Service Provider with the operational asset physically located somewhere in Atlanta, Georgia
  - The trail of logical and physical infrastructures blurs the issue of which allies share the same infrastructures.

Issue 2

- If Green is sharing information infrastructures with Red does that make them a valid target?
  - Great question
  - Question of law and politics
  - Shared infrastructures may or may not be known at the onset of hostilities
  - The reasonable answer is, “It depends”
  - The final answer is “I’m not a lawyer”

Blue on Blue v.2

- Blue intelligence agency uses Blue civilian infrastructures
- Examples of this could be a worm or virus showing up anywhere Blue but at the target

Issue 3

- Why not worry about the legal concerns?
  - National security in most countries trumps protections against government intrusions
  - Projection of power in the kinetic domain has always been fraught with risk
  - The risk conundrum has only been lightly scratched at this point

Conclusions

- Current targeting practices include a feedback loop to assess
- The command and control (C2) of cyber fires needs to be fully integrated with health of the C2 apparatus taken into account
- Area of operations constructs are going to need further defined and assessed
- Functional issues of staff controls will need to be addressed
- Mapping and tools for situational awareness across all domains will have to be utilized

After the paper was written

- Patterns of fratricide or risk of fratricide over the past months
- Security operations centers shutting off mission critical services because they aren't secure
- Incident responders "killing the machine" to keep compromise to a minimum, but putting operational assets at risk in the field
- Intelligence agencies not providing relevant and timely information on target and attacker (long history of this)
- Allies not communicating on their activities in cyberspace degrading, disrupting and putting each other in jeopardy
- Unexpected consequences of cyber capabilities jumping from targets creating collateral damage

Questions?

PURDUE UNIVERSITY

CYBERFORENSICS LABORATORY

Cyber Fratricide

CERIAS®

Center for Education and Research in Information Assurance and Security