Ministry of Defence

Adopting Botnet Herders' Techniques in Military C2 Systems

Netherlands Defence Academy
Tim Grant
tj.grant@nlda.nl

ICCRTS 19 Jun 12

Overview

Goal:

- To identify botnet herders' C&C techniques that could be adopted in military C2 systems

Outline:

- Introduction
- Military C2
- Botnet C&C
- Comparison
- Conclusions

Introduction (1)

My qualifications:

- BSc Aeronautical Engineering, Bristol, UK
- Defence Fellowship (Masters), Brunel, UK
- PhD Artificial Intelligence, Maastricht, NL

My experience:

- 1966-87: Royal Air Force officer, UK & SG
- 1987-2004: Consultant, Atos Origin, NL
- 2001-09: Professor, U. Pretoria, ZA (20%)
- 2004-12: Professor, NLDA, Breda, NL (50%):
  - *Teaching*: Communication, Information & C2 Systems
  - *Research*: operational ICT & communications
  - *Management*: team of 7,5 lecturers

Introduction (2)

My C4I systems team's research:

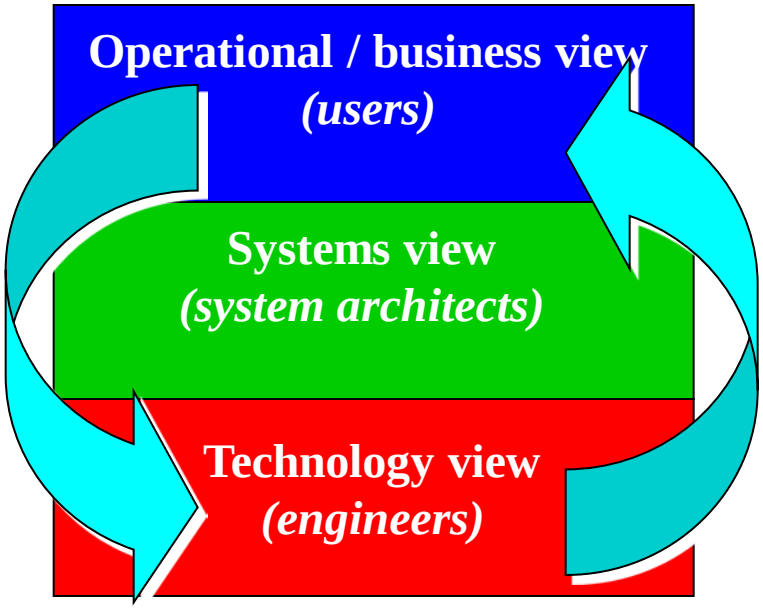
- Focused on:
  - Information & Communication Technology (ICT)
  - Network Enabled C2 Systems (NECS)
  - Offensive cyber operations

- Active research into:
  - Actor-network analysis of C2 simulator (PhD)
  - Tools & technologies for offensive cyber ops
  - Social media in C2
  - Information sharing with coalition partners:
    - › Cultural influences (PhD)
    - › Service-oriented computing (PhD)
  - Dynamic workflows for synchronizing C2 (PhD)

Introduction (3)

My research approach:

Operational needs impose requirements on technology
(eg cyber)



New ICTs make possible new types of operation
(eg social media)

My time horizon:

Introduction (4)

Research Question:

Are there operational advantages to be gained by adopting techniques from botnet C&C in military C2 systems?

and in particular:

What would we have to do to operate C2 systems over the "dirty" Internet?

Military C2 (1): operational environment

Four domains:

- Physical
- Information
- Cognitive
- Socio-organizational

Interactions between actors:

- Mostly in physical domain

Key determinants of action:

- Terrain
- Technical capabilities

Military C2 (2): threats & responses

Threats:

- Opposing forces
- To C2 systems:
  - Destruction or disruption of C2 system
  - Denial of access to or disclosure of information

Responses:

- Information security principles:
  - Confidentiality, Integrity, Availability (CIA)
  - Authenticity & Non-Repudiation
- Primarily defensive:
  - “Air-gapping”

Military C2 (3): industrial-age C2

Organizational structure:

- Traditionally hierarchical (“Machine Bureaucracy”)

Mintzberg, 1980

Decision making:

- Centralized

Information flow:

- Formal
- Up & down hierarchy

Galbraith, 1974; 1977; 2008

Military C2 (4): information-age C2

Organizational structure:

- Edge (“Professional Ad-hocracy”)

Alberts & Hayes, 2003

Decision making:

- Centralized goal selection
- Decentralized execution
- Mutual adjustment; self-synchronization

Nissen, 2005

Information flow:

- Formal & informal
- Up & down, across, and between hierarchies

Botnet C&C (1): operational environment

Four domains again

Interaction between actors:

- Mostly in information domain
- Social engineering in cognitive domain

Key determinants of action:

- Cyberspace is man-made:
  - Topology / connectivity
  - IP address equivalent to lat-long:
    - Easily changed – no inertia
- Free from physical & legal constraints

Botnet C&C (2): threats & responses

Threats:

- Target's developer & system administrator
- OS, FW, AV, IDS & application developers
- Rival botnet herders
- Law enforcement authorities

Responses:

- Exploit vulnerabilities
- Encrypting malware
- Multiple versions of malware
- Remove rival botnets
- Exchange techniques via dark fora & chat channels

Botnet C&C (3): topologies & techniques (1/2)

Botnet generations:

- Open-source
- Kit-based
- Specialized

Czosseck et al, 2011

Botnet topologies:

- Centralized via IRC
- Peer-to-peer (P2P) networks:
  - Random graphs
  - Small worlds
  - Scale-free

Li et al, 2009

Zeldanoo & Manaf, 2009

Wang et al, 2010

Botnet C&C (3): topologies & techniques (2/2)

Communication technologies:

- IRC protocol (popular)
- HTTP
- Twitter

Kartaltepe et al, 2010

Obfuscation techniques:

- Encryption
- Onion routing
- Lookup resilience
- Redundant C&C servers
- Intermittent C&C; calling home
- IP & domain fluxing (cf. frequency-hopping)

Damballa, 2009a/b

Comparison (1)

	Military C2	Botnet C&C
Closed loop	Yes (OODA)	Yes
Tempo	Yes	Yes
Domains	Physical, information, cognitive, social	Information (cyberspace), cognitive
Supervisory control	Commander	Botnet herder
Direct control	Command team & C2 system	C&C servers
Process under control	Subordinate units	Zombie-hosted bots
Targets	Opposing forces	Target systems

Comparison (2)

	Military C2	Botnet C&C
Environment	Terrain, objects (natural & man-made), weather, etc	Open Internet, computing systems, routers, networks
Infostructure	Dedicated; air-gapped from Internet	Embedded in “dirty” Internet
Organizational structure	Hierarchy -> Edge	Centralized (scale-free); P2P (small worlds); unstructured (random graphs)
Threats	Opposing forces	Developers; system administrators; rival botnet herders; law enforcement
Responses	Air-gapping; security classification; need-to-know; policies; SOPs; encryption	Stealth; obfuscation; creating multiple bot varieties

Comparison (3)

	Military C2	Botnet C&C
Legal constraints	National & international law; national boundaries; jurisdications	None
Physical constraints	Natural, national & man-made barriers; geography; metric distance; inertia of objects; vehicle speed	None Except for diurnal rhythm of users of some zombie & target systems

Comparison (4)

Does C2 = C&C?

- Both closed loop & emphasize tempo
- Both have overall commander
- Both contend with intelligent adversaries
- Subordinates differ
- => Similar in character

Comparison (5)

Botnet herder has easier job in terms of:

- No physical limitations (inertia, distance, speed)
- No legal constraints

But botnet operates in “dirty” environment:

- Open Internet
- Surrounded by targets
- Must “hide in plain sight”
- Must secure assets from malware:
  - Like everyone else
- Confronted with rival botnet herders

Comparison (6)

Military C2 systems “air-gapped”:

- Cannot “live off the land”
- Logistics footprint
- Cut off from useful open-source information:
  - CNN, Google, social networks
- “Air-gapping” is leaky:
  - Updates
  - Careless users
  - USB as WMD

Conclusions (1)

Operational advantages of botnet techniques?

- Enables agility, “living off land”, & reduced footprint:
  - Use existing infostructure
  - Bring Your Own Device
- Integrate formal & open-source information:
  - Use public databases
  - C2 systems as mash-ups:
    - eg Google Maps, Ushahidi, etc for SA
    - eg social media as comms channel
- Simplify interoperability with non-military partners
- Manouevre & stealth as cyber defence:
  - Instead of fortress thinking (FW, AV, IDS)

Conclusions (2)

Botnet herders further than military C2:

- NML 4? TRL 6?
- Developed range of techniques:
  - Stealth, obfuscation, fluxing, etc.

Made *prima facie* case for adopting their techniques

Recommendation:

- Perform military C2 proof-of-concept (CD&E)

Any Questions?

(Up to 12:00 NL, 29 June 2012:)
tj.grant@nlda.nl

(From 1 July 2012 onwards:)
tim.grant.work@gmail.com

Mob: +31 (0)638 193 749
SkypeID: t.j.grant