


## InfraGard: A Potential Model for Combatting Cybercrime in Europe



INTERNATIONAL CYBER THREAT TASK FORCE  
**ICTTF**  
www.icttf.org

*Cyber Threat Summit  
Dublin Ireland  
July 5, 2011*

Chuck Georgo  
Executive Director  
**NOWHERETO HIDE.ORG**  
**TeamInfoSec**

---

---

---

---

---

---

---

---

### About me...

- 30+ years IT design, development, and delivery
- Positions:
  - Associate, TeamInfoSec, Dublin
  - Executive Director, NOWHERETO HIDE.ORG
  - First Vice President/Programs Director, InfraGard Maryland Members Alliance
  - Chairman, Security and Privacy Committee, Integrated Justice Information Systems Institute
- Core expertise
  - Solve tough problems
  - Get more done/save money
  - Process improvement
  - Build intelligence capability
  - Apply technology for public safety/national security

6/30/2011 2

---

---

---

---

---

---

---

---

### Experience brought to bear...

- U.S. Naval Security Group
- National Security Agency
- Naval Criminal Investigative Service
- Federal Bureau of Investigation
- U.S. Postal Inspection Service
- U.S. Intelligence Fusion Centers (many)
- Illinois State Police
- Microsoft Corporation
- New York City Police Department
- North Atlantic Treaty Organization
- Canadian Intelligence Service Ontario
- Royal Canadian Mounted Police
- 200+ U.S. Law Enforcement Agencies



Systems Engineer/Architect (DEFINE)  
Chuck Georgo  
Program and Project Manager (MANAGE)  
Human Performance Technologist (IMPLEMENT)

6/30/2011 3

---

---

---

---

---

---

---

---

### What are we facing?

- Corporate espionage
- Commerce interruption
- Financial fraud
- Human trafficking
- Child pornography
- Illegal immigration
- Drug trafficking



6/30/2011

---

---

---

---

---

---

---

---

### Real World Consequences

- Loss of revenues
- Public embarrassment
- Loss of faith/trust
- Loss of jobs
- Exploited women and children
- More dangerous communities



6/30/2011

---

---

---

---

---

---

---

---

### Cyber as Key Enabler

- EU Organised Crime TA - 2011

Internet technology has now emerged as a key facilitator for the vast majority of online-organised crime activity. In addition to the high-tech crimes of cybercrime, payment card fraud, the distribution of child abuse material, and audio visual piracy, extensive use of the Internet for underground chat, blog, forums, electronic mail, distributing the recruitment and marketing of recruits to human beings (THB), the facilitation of illegal immigration, the supply of counterfeit commodities, trafficking in endangered species, and many other criminal activities, it is also widely used as a secure communication and money laundering tool by criminal groups.

6/30/2011

---

---

---

---

---

---

---

---

### The Adversaries

- Organized
- Motivated
- Determined
- Agile
- Tech savvy
- Networked



Organized crime is changing and becoming increasingly diverse in its methods, group structures, and impact on society. A new criminal landscape is emerging, marked increasingly by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors, and aided, in particular, by sophisticated tools used on the Internet.

6/30/2011 7

---

---

---

---

---

---

---

---

### Bottom Line

*It will take a network to defeat a network...*

6/30/2011 8

---

---

---

---

---

---

---

---

### Introduction to U.S. InfraGard



6/30/2011 9

---

---

---

---

---


---

---

---

### U.S. InfraGard Program

- Public-private partnership
- Established by U.S. Federal Bureau of Investigation (FBI) in 1996
- Initial focus was cybercrime
- Expanded in 1998 to address terrorism, intelligence and general crime matters
- 42,000+ members
- 80+ chapters



6/30/2011 10

---

---

---

---

---

---

---

---

### InfraGard Objectives

- Five objectives:
  1. Increased information sharing between critical infrastructure owners/operators and the FBI.
  2. Increase information sharing among critical infrastructure owners/operators themselves.
  3. Trusted mechanism for communicating threat advisories, alerts, and warnings.
  4. Stronger liaison with law enforcement and homeland security agencies.
  5. Forum for critical infrastructure protection education and training

6/30/2011 11

---

---

---

---

---

---

---

---

### InfraGard Structure

- Two tier structure
  - National level non-profit corporation – *InfraGard National Members Alliance*
  - Local/state level non-profit groups



6/30/2011 12

---

---

---

---

---

---

---

---

### InfraGard Structure

- **National** level non-profit corporation:
  - Owns relationship with FBI in Washington D.C.
  - Establishes operating policy and guidance
  - Supports local chapter activities
- **Local/State** level organizations (chapters):
  - Has direct relationship with local FBI field office
  - Recruits critical infrastructure owners/operators and law enforcement/homeland security members
  - Holds education and training events
  - Facilitates information sharing among members

6/30/2011 13

---

---

---

---

---

---

---

---

### Maryland Chapter Website



6/30/2011 14

---

---

---

---

---

---

---

---

### Joint Critical Infrastructure Partnership

- Brings the U.S. Department of Homeland Security (DHS) into partnership
- Establishes stronger link to local intelligence fusion centers
- Blends FBI objectives with DHS National Infrastructure Protection Plan (NIPP)



6/30/2011 15

---

---

---

---

---

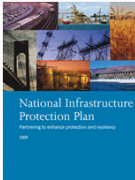
---

---

---

### DHS NIPP Objectives

- Share information about terrorist threats and other hazards with partners;
- Build partnerships to implement protection programs;
- Implementing a long-term risk management program; and
- Coordinate efficient use of resources for protection, restoration, and recovery.



6/30/2011 16

---

---

---

---

---

---

---

---

### NIPP – Critical Infrastructures



6/30/2011 17

---

---

---

---

---

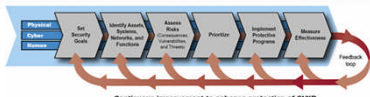
---

---

---

### NIPP – Risk Management Framework

- Emphasis placed on three *horizontal* threats across all critical infrastructure sectors:
  - Physical threats
  - Cyber threats
  - Human threats



6/30/2011 18

---

---

---

---

---


---

---

---

### European Commission CIIP

- Five pillars:
  1. Preparedness and prevention;
  2. Detection and response;
  3. Mitigation and recovery;
  4. International cooperation and promotion of EU priorities internationally; and
  5. Criteria for the ICT sector to support implementation.



6/30/2011 19

---

---

---

---

---

---

---

---

### The Missing Key

- Para 3.4.2 Need for a new European governance model for CIIs:

To address this governance problem public-private partnerships (PPPs) have emerged at the national level as the reference model. However despite the consensus that PPPs would likely be desirable on a European level, European PPPs have not materialized so far. A Europe-wide multi-stakeholder governance framework, which may include an enhanced role of ENISA, could foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures. This framework would bridge the gap between national policy-making and operational reality on the ground.

6/30/2011 20

---

---

---

---

---

---

---

---

### Proposal:

***Implement an InfraGard-like network in Europe to help combat cybercrime...***

***...to serve as Europe's public-private partnership called for in the CIPP.***

6/30/2011 21

---

---

---

---

---

---

---

---

### What would it look like?

- Build on efforts of ICTTF
- Adapt features U.S. InfraGard model
- Begin as **private**-sector information sharing platform
- Start small, then grow—crawl, walk, run
- Identify 3-5 country level cells (chapters)
- Establish core leadership team
- Establish trusted sharing platform
- Expand from there...

6/30/2011 22

---

---

---

---

---

---

---

---

### Core Enablers

- International Cyber Threat Task Force
- Irish Cyber Crime Task Force
- European Commission – *European Programme for Critical Infrastructure Protection*
- European Network and Information Security Agency

6/30/2011 23

---

---

---

---

---

---

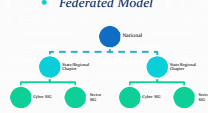
---

---

### Can it work in Europe?


#### U.S. InfraGard

- One country
- One lead gov't agency
- One set of laws
- One central body
- *Federated Model*



#### EUGuard

- Many countries
- Many sets of laws
- Many government agencies
- No central body
- *Decentralized Model?*



6/30/2011 24

---

---

---

---

---

---

---

---



**Next Steps**

- Establish interest in Ireland
- Convene planning meeting
- Develop concept for operations
  - Pilot objectives
  - Member vetting criteria
  - Rules of engagement
  - Measures of effectiveness
- Implement trusted sharing environment

6/30/2011 25

---

---

---

---

---

---

---

---

**Thank you**

Chuck Georgo  
Executive Director,  
**NOWHERE TO HIDE.ORG**

Contact Information:  
Email: [chuck@nowheretohide.org](mailto:chuck@nowheretohide.org)  
U.S. cell: +1-410-903-6289  
Éire cell: 085 1039081  
Skype: chuckgeorgo  
Twitter: chuckgeorgo



**TeamInfoSec**  
[www.teaminfosec.com](http://www.teaminfosec.com)

6/30/2011 26

---

---

---

---

---

---

---

---