Critical Information Infrastructure Protection and CIRT

Raj Kumar

Critical Information Infrastructure Protection and CIRT

- What is CIIP?
- Measurement Impact of Critical Information Infrastructure
- Current Threat Landscape
- Need for National CIRT
- Functions and requirements
- Collaborations among CIRTS

What is CIIP?

Critical Information Infrastructure Protection (CIIP) is defined as those assets (real and virtual), systems and functions that are vital to the nations that their incapacity or destruction would have a devastating impact on:

- National economic strength.
- National image.
- National defence and security.
- Government capability to functions.
- Public health and safety.

CIIP Sectors are:

- National Defence & Security
- Banking & Finance
- Information & Communications
- Energy
- Transportation
- Water
- Health Services
- Government
- Emergency Services
- Food & Agriculture

Measurement Impact of Critical Information Infrastructure

Is there a case for a National Action?	• Identify a national policy on cybersecurity/CIIP. • Identify a case for national action on cybersecurity/CIIP.
Who are the participants in the National Response?	• Identify key government ministries and agencies with leadership responsibilities in cybersecurity/CIIP and describe their roles. • Identify key other participants with responsibilities in cybersecurity/CIIP and describe their role(s).
Is there an organization structure for Cybersecurity/CIIP)?	• Identify organizational structures to be used for the development of cybersecurity/CIIP policy. • Identify organizational structures to be used for ongoing cybersecurity/CIIP operations.
Is there a collaboration model between Government-Private Sector?	• Identify objectives and structures for trusted government/private sector collaboration.
Is there Incident Management Capabilities?	• Identify location within government of the incident management capability function. • Identify and prioritize objectives of the incident management capability function.
What are the current Legal Infrastructure?	• Identify objectives for updating the legal infrastructure related to cybercrime. • Identify objectives for updating other elements of the legal infrastructure.
How is the Culture of Cybersecurity developed?	• Identify and prioritize objectives for building a national culture of cybersecurity.

https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-self-assessment-toolkit.pdf

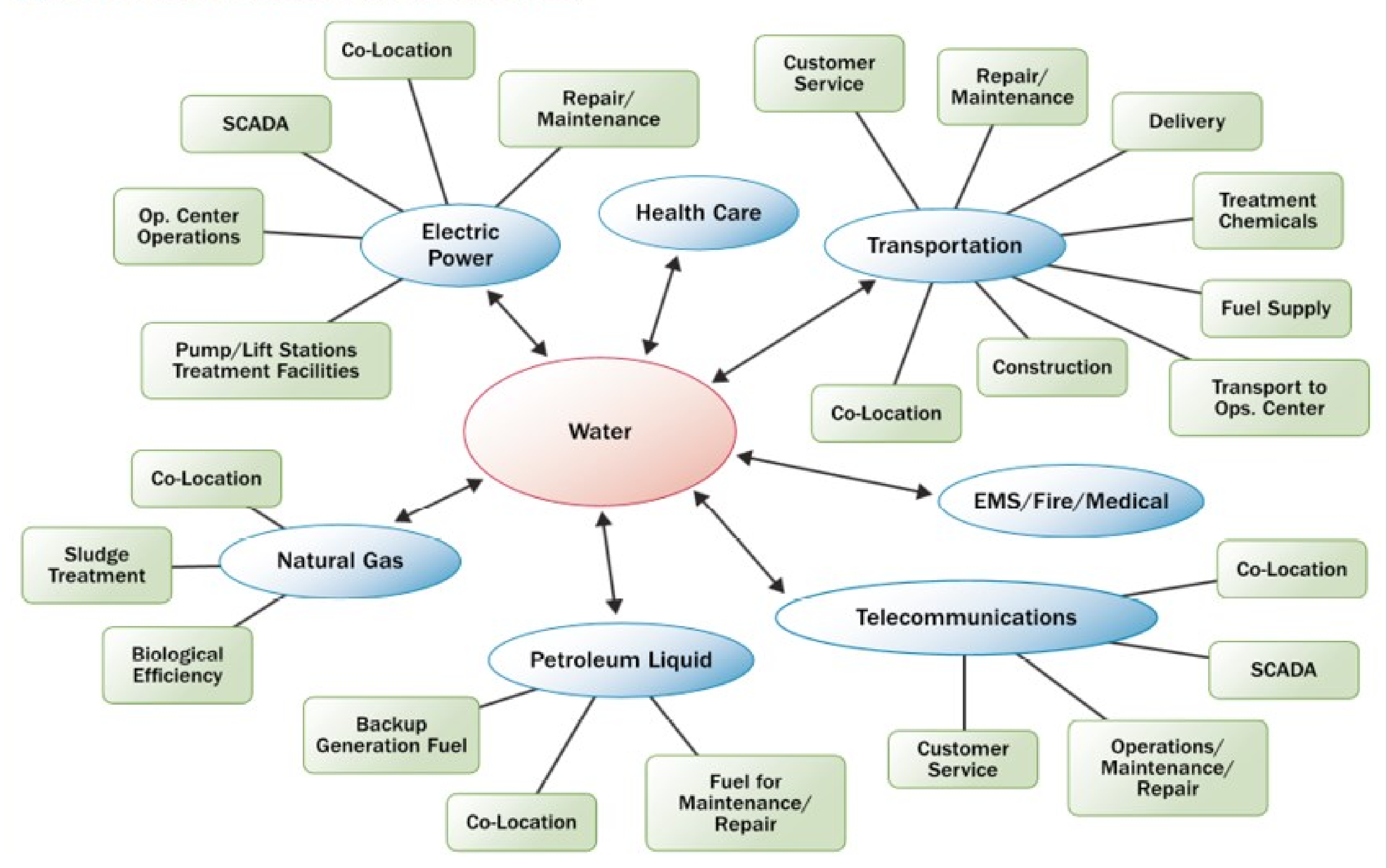
Current Threat Landscape

- Increasing exponentially in volume and variation
- Everyone is exposed to cyber threats
- Main motive is monetization
- Crimeware aims for profit
- State of the art and advanced threat agents
- Hacking tools widely available and offered “as a service”
- Maturity of defenders have increased too

Threats to Critical Infrastructure

The high degree of interdependency between critical infrastructure sector means failure in one sector can propagate into others

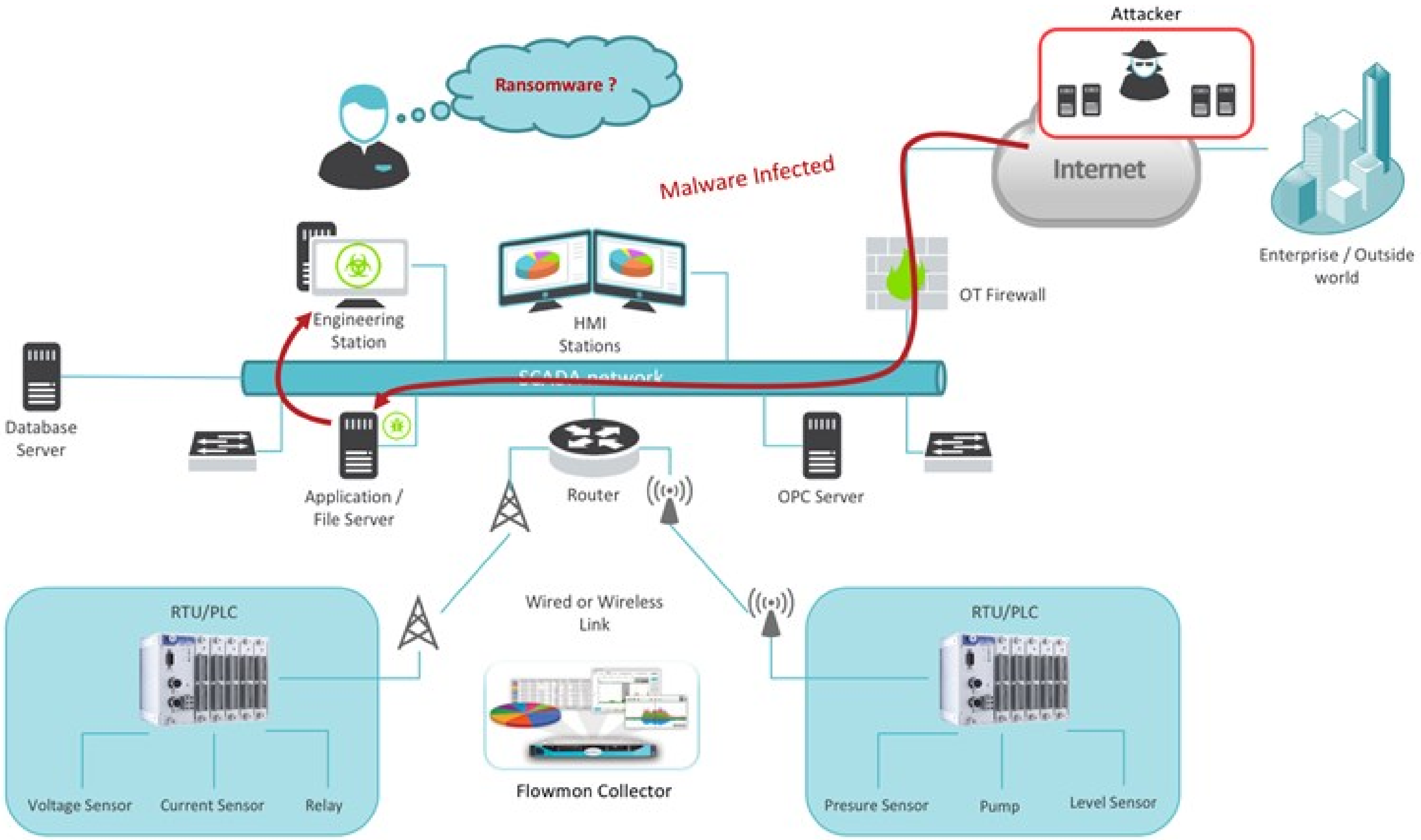
Figure 3-2: Interdependencies with the Water Sector



https://www.hsaj.org/resources/uploads/2016/05/Image76839.png

SCADA Systems

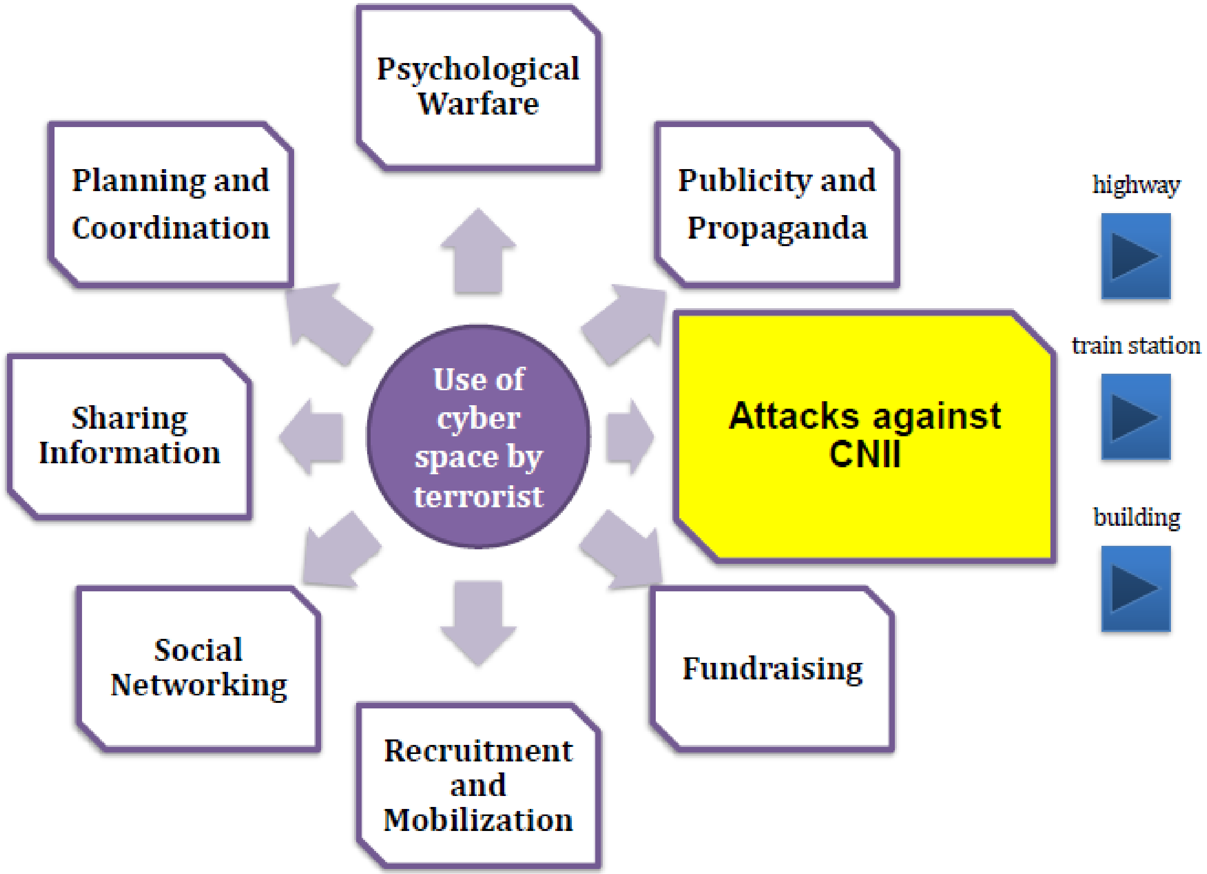
The interconnection of Supervisory Control And Data Acquisition (SCADA) systems to corporate networks & their reliance on common operating platforms and remote excess - exposing SCADA systems to vulnerabilities



https://www.flowmon.com/getattachment/Blog/Network-visibility-in-the-SCADA-ICS-environment/figure1.png.aspx?lang=en-GB&width=800&height=448

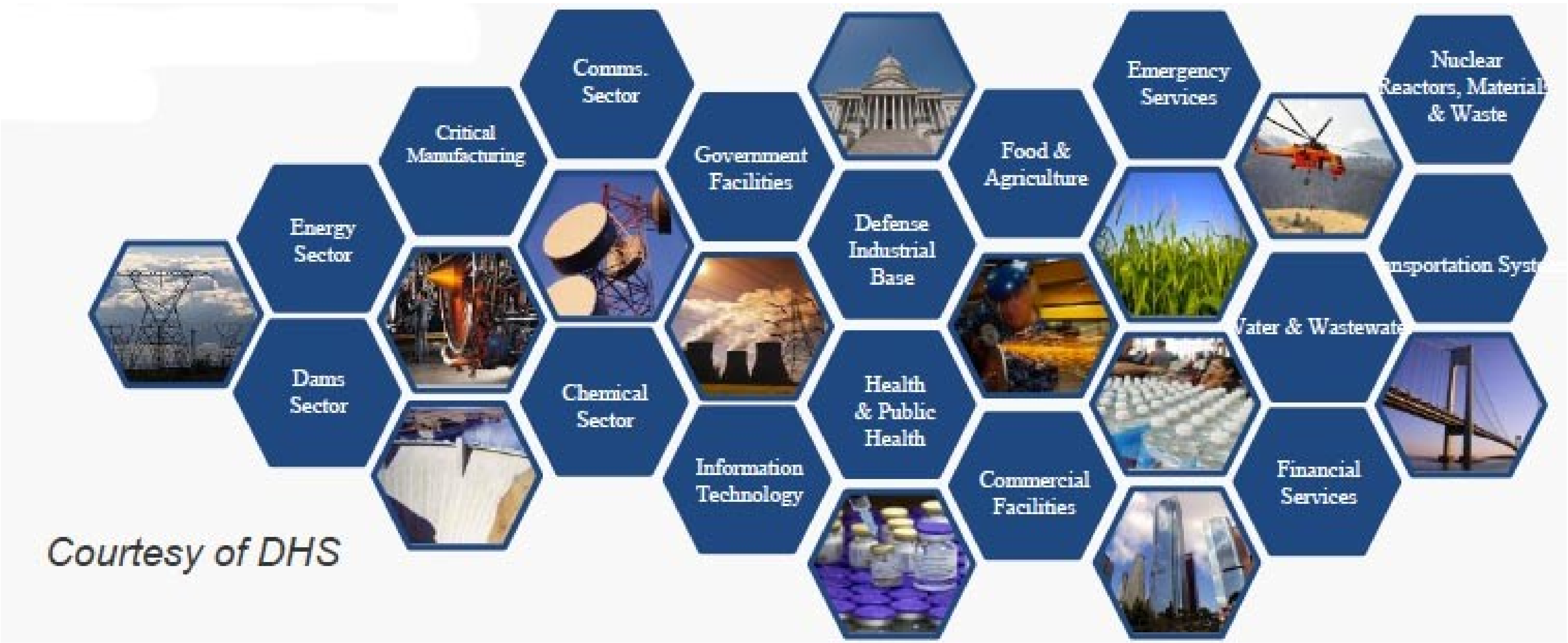
Attacks against Critical Sector

The perpetrator may utilize the cyberspace for conducting cyber attacks on critical national information infrastructure facilities



https://www.slideshare.net/CommonwealthTelecommunications/session-32-zahri-hj-yunos

Cyber Attack Potential Target



Courtesy of DHS

Attackers today

- Abusing unsecured components to mobilize a very large attack potential. This capacity that has been demonstrated by means of DDoS attacks by infected IoT devices.
- Successfully launching extortion attacks that have targeted commercial organisations and have achieved very high levels of ransom and high rates of paying victims.
- Demonstrating very big impact achieved by multi-layered attacks to affect the outcome of democratic processes at the example of the US elections.
- Operating large malicious infrastructures that are managed efficiently and resiliently to withstand takedowns and allow for quick development and multi-tenancy.

http://www.diariodigitalcolombiano.com/un-monton-de-hackers-se-disponen-a-tumbar-los-populares-routers-domesticos/

Cyber Attacks today

- More cyber criminals than cyber cops
- Criminals feel safe committing crimes from the privacy of their homes
- Cyber threats may be perpetrated with little cost and few resources.
- Brand new challenges for law enforcement

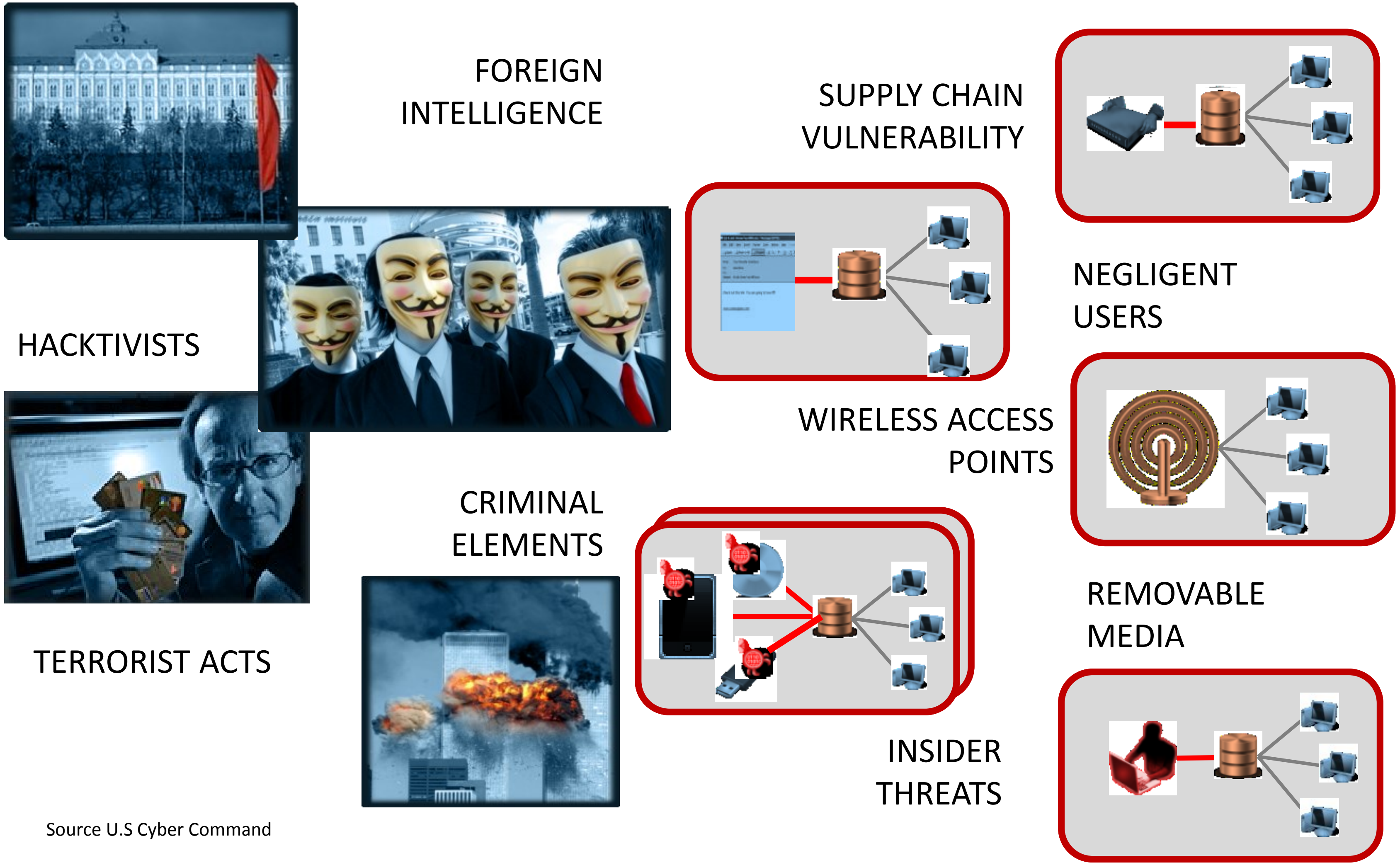
  - Most are not trained in technologies

  - Internet crimes span multiple jurisdiction

Threat Actors

THREAT ACTORS

THREAT VECTORS



FOREIGN INTELLIGENCE

HACKTIVISTS

CRIMINAL ELEMENTS

TERRORIST ACTS

Source U.S Cyber Command

SUPPLY CHAIN VULNERABILITY

NEGLIGENT USERS

WIRELESS ACCESS POINTS

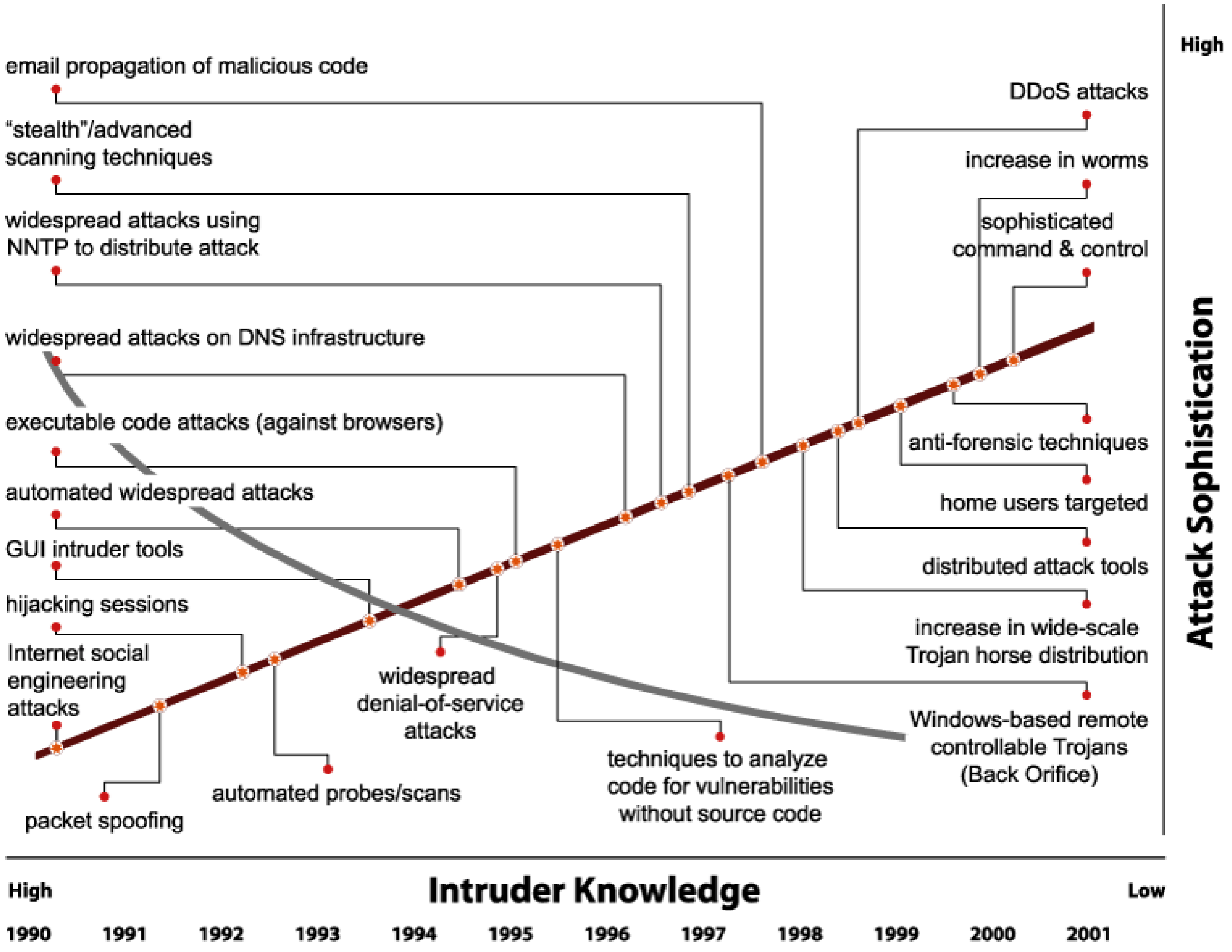
REMOVABLE MEDIA

INSIDER THREATS

Types of Cyber Threats

Type	Motivation	Target	Method
Cyber War	Military or political dominance	Critical infrastructure, political and military assets	Attack, corrupt, exploit, deny, co-joint with physical attack
Cyber Espionage	Gain of intellectual Property and Secrets	Governments, companies, individuals	Advanced Persistent Threats
Cyber Crime	Economic gain	Individuals, companies, governments	Fraud, ID theft, extortion, Attack, Exploit
Hacking	Ego, personal enmity	Individuals, companies, governments	Attack, Exploit
Hactivism	Political change	Governments, Companies	Attack, defacing
Cyber Terrorism	Political change	Innocent victims, recruiting	Marketing, command and control, computer based violence

Technical knowledge vs tools

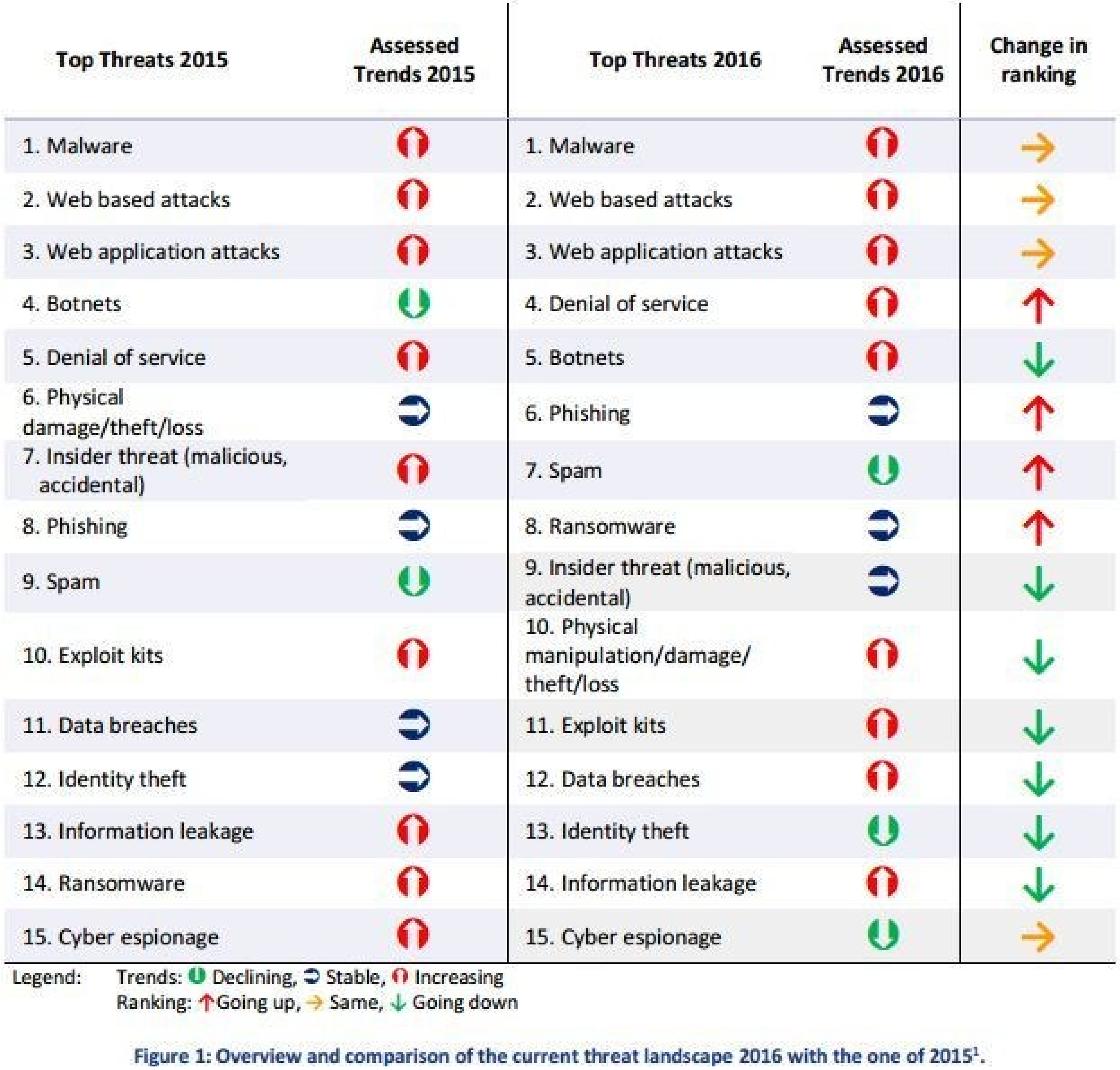


http://users.atw.hu/denialofservice/images/0131475738/graphics/03fig02_alt.gif

Modern Weapon Economics

	What does a stealth bomber cost?	**$1.5 to $2 billion**
	What does a stealth fighter cost?	**$80 to $120 million**
	What does an cruise missile cost?	**$1 to $2 million**
	What does a cyber weapon cost?	**$300 to $50,000**

ENISA’s Top Threat 2015 vs 2016



Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	⇧	1. Malware	⇧	→
2. Web based attacks	⇧	2. Web based attacks	⇧	→
3. Web application attacks	⇧	3. Web application attacks	⇧	→
4. Botnets	⇩	4. Denial of service	⇧	↑
5. Denial of service	⇧	5. Botnets	⇧	↓
6. Physical damage/theft/loss	⇨	6. Phishing	⇨	↑
7. Insider threat (malicious, accidental)	⇧	7. Spam	⇩	↑
8. Phishing	⇨	8. Ransomware	⇨	↑
9. Spam	⇩	9. Insider threat (malicious, accidental)	⇨	↓
10. Exploit kits	⇧	10. Physical manipulation/damage/ theft/loss	⇧	↓
11. Data breaches	⇨	11. Exploit kits	⇧	↓
12. Identity theft	⇨	12. Data breaches	⇧	↓
13. Information leakage	⇧	13. Identity theft	⇩	↓
14. Ransomware	⇧	14. Information leakage	⇧	↓
15. Cyber espionage	⇧	15. Cyber espionage	⇩	→

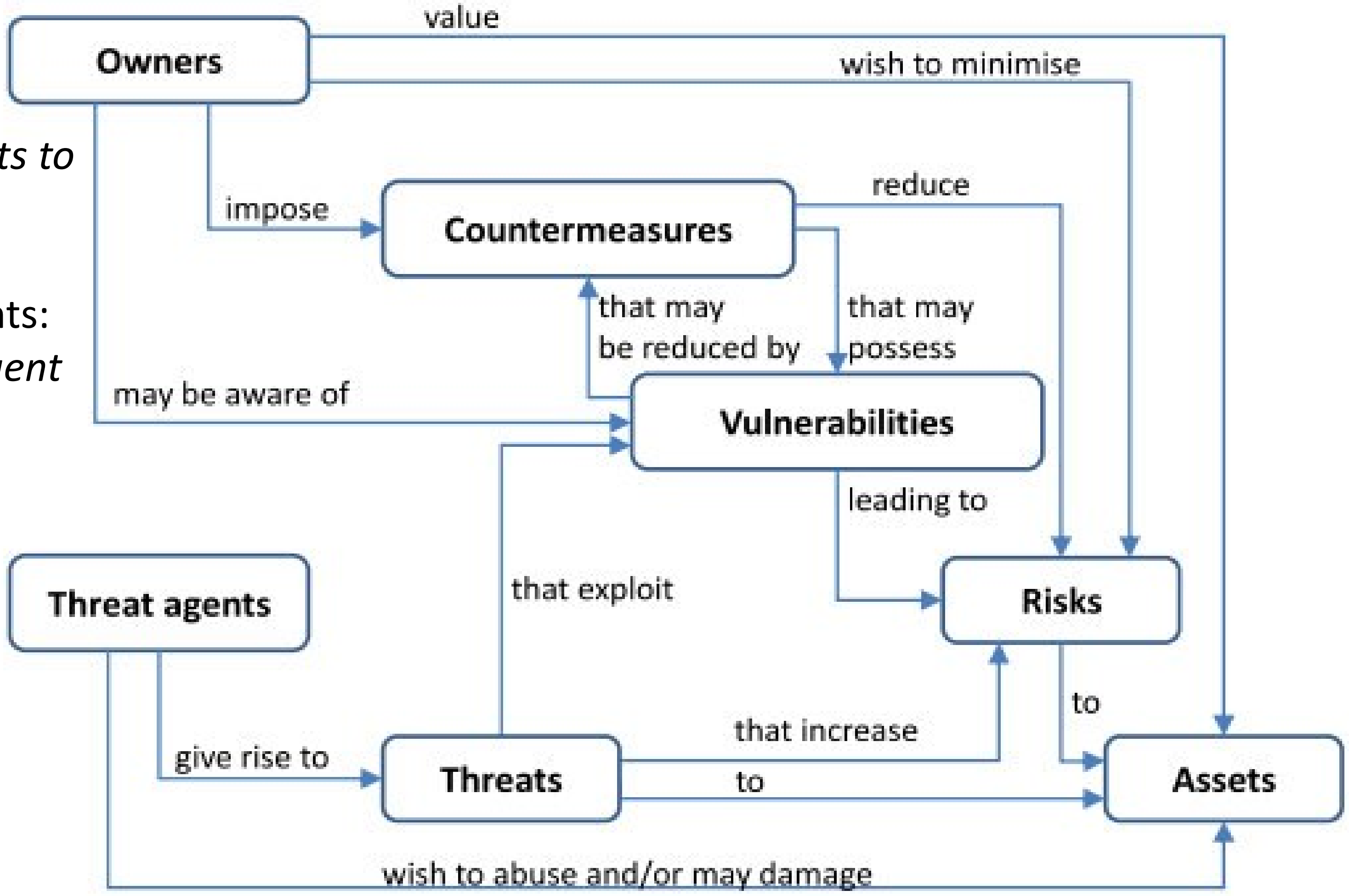
Legend: Trends: ⇩ Declining, ⇨ Stable, ⇧ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Figure 1: Overview and comparison of the current threat landscape 2016 with the one of 2015[1].

Threat, Risk and Impact

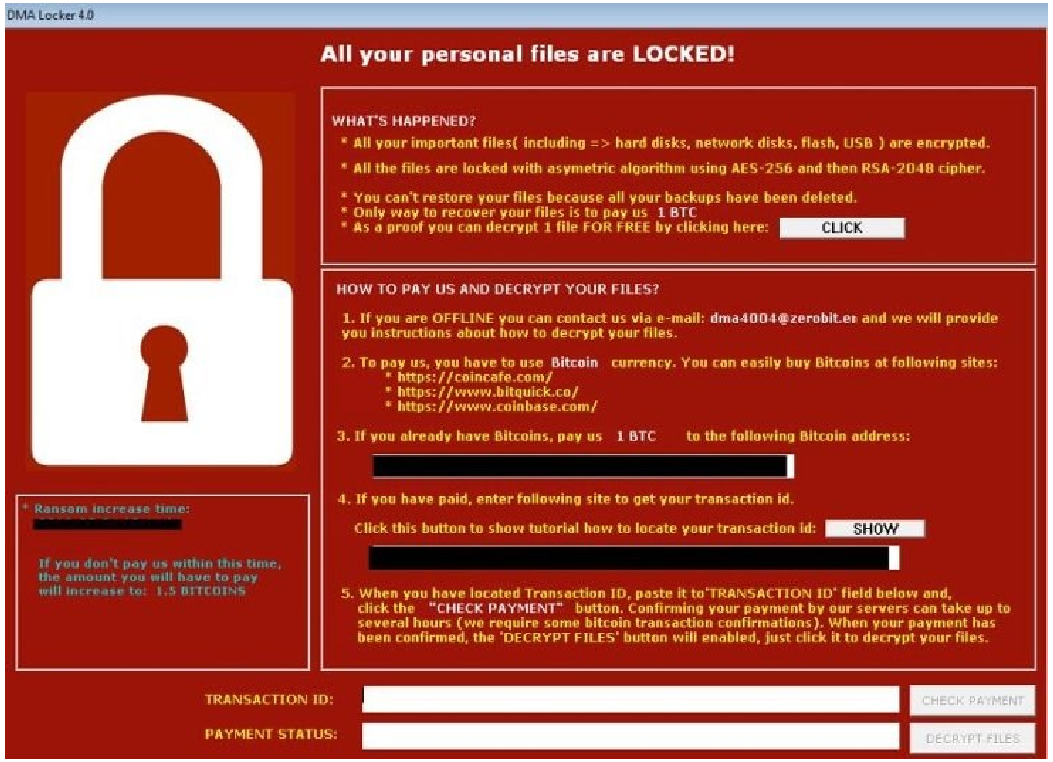
ISO 27005 - *"Threats abuse vulnerabilities of assets to generate harm for the organisation"*.

Risk can be considered using the following elements: **Asset** (*Vulnerabilities, Controls*), **Threat** (*Threat Agent Profile, Likelihood*) and **Impact**.



Malware

- Malware-as-a-Service
- IoT Malware
- Mobile Malware
- Ransomware
- Information stealers
- Trojans
- PUP (Potentially unwanted Program)
- Droppers
- Command and Control
- Keylogger/Phishing Based
- Backdoor
- DDoS Malware
- RAT
- Worms
- Virus
- Adware/Spyware



DMA Locker 4.0

All your personal files are LOCKED!

WHAT'S HAPPENED?

* All your important files(including => hard disks, network disks, flash, USB) are encrypted.

* All the files are locked with asymetric algorithm using AES-256 and then RSA-2048 cipher.

* You can't restore your files because all your backups have been deleted.
* Only way to recover your files is to pay us 1 BTC
* As a proof you can decrypt 1 file FOR FREE by clicking here: CLICK

HOW TO PAY US AND DECRYPT YOUR FILES?

1. If you are OFFLINE you can contact us via e-mail: dma4004@zerobit.er and we will provide you instructions about how to decrypt your files.

2. To pay us, you have to use Bitcoin currency. You can easily buy Bitcoins at following sites:
   * https://coincafe.com/
   * https://www.bitquick.co/
   * https://www.coinbase.com/

3. If you already have Bitcoins, pay us 1 BTC to the following Bitcoin address:

   [redacted]

4. If you have paid, enter following site to get your transaction id.

   Click this button to show tutorial how to locate your transaction id: SHOW

   [redacted]

5. When you have located Transaction ID, paste it to'TRANSACTION ID' field below and, click the "CHECK PAYMENT" button. Confirming your payment by our servers can take up to several hours (we require some bitcoin transaction confirmations). When your payment has been confirmed, the 'DECRYPT FILES' button will enabled, just click it to decrypt your files.

* Ransom increase time:
[redacted]

If you don't pay us within this time, the amount you will have to pay will increase to: 1.5 BITCOINS

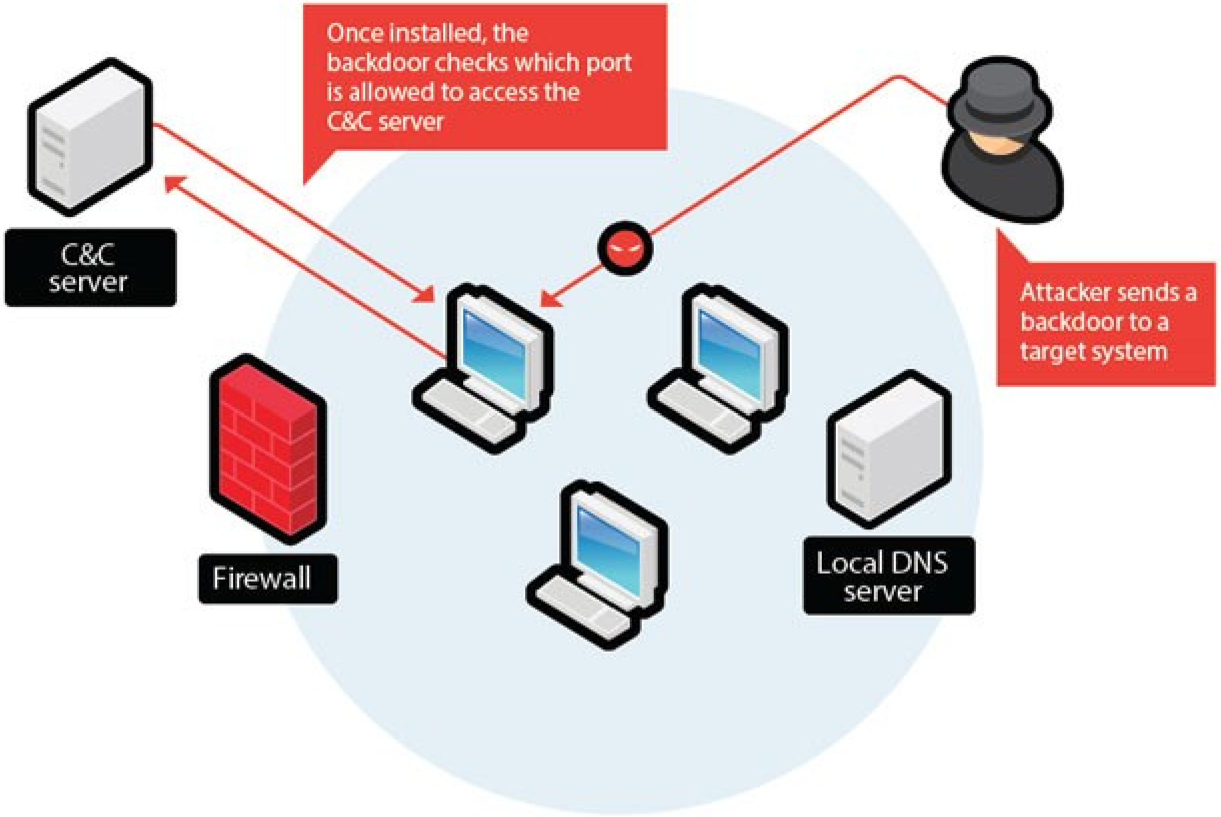
TRANSACTION ID: CHECK PAYMENT

PAYMENT STATUS: DECRYPT FILES

https://www.incapsula.com/web-application-security/malware-detection-and-removal.html

Web-based Attacks

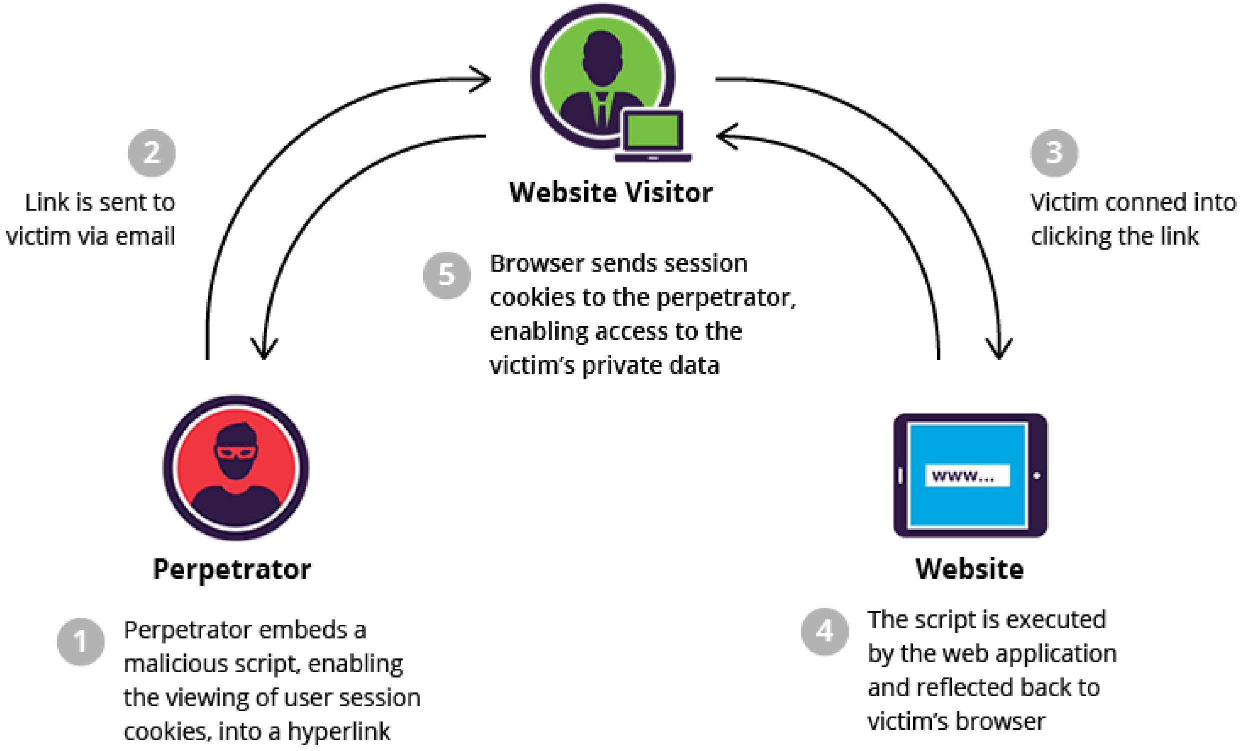
- Drive-by-attacks
- Redirection
- Water-holing attack
- Web browser and server exploits
- Browser extension/plug-in attacks
- Man in the browser attack
- Backdoors
- Spyware
- Search Engine Optimisation (SEO) compromise
- Drive-by-downloads
- Malicious IPs/URLs


Once installed, the backdoor checks which port is allowed to access the C&C server
C&C server
Attacker sends a backdoor to a target system
Firewall
Local DNS server

https://commons.wikimedia.org/wiki/File:Backdoor_%D1%85%D0%B0%D0%BB%D0%B4%D0%BB%D0%B0%D0%B3%D0%B0.jpg

Web Application attack

- Local File Inclusion
- SQL Injection
- Cross Site Scripting (XSS)
- Remote File Inclusion
- PHP Injection
- Transport layer weaknesses
- Information Leakage
- Brute Force attack
- Input validation/handling
- Predictable Resource Allocation
- Directory Indexing
- Insufficient Password Protection
- Cross Site Request Forgery
- Abuse of Functions



Website Visitor

Perpetrator

Website

1 Perpetrator embeds a malicious script, enabling the viewing of user session cookies, into a hyperlink

2 Link is sent to victim via email

3 Victim conned into clicking the link

4 The script is executed by the web application and reflected back to victim's browser

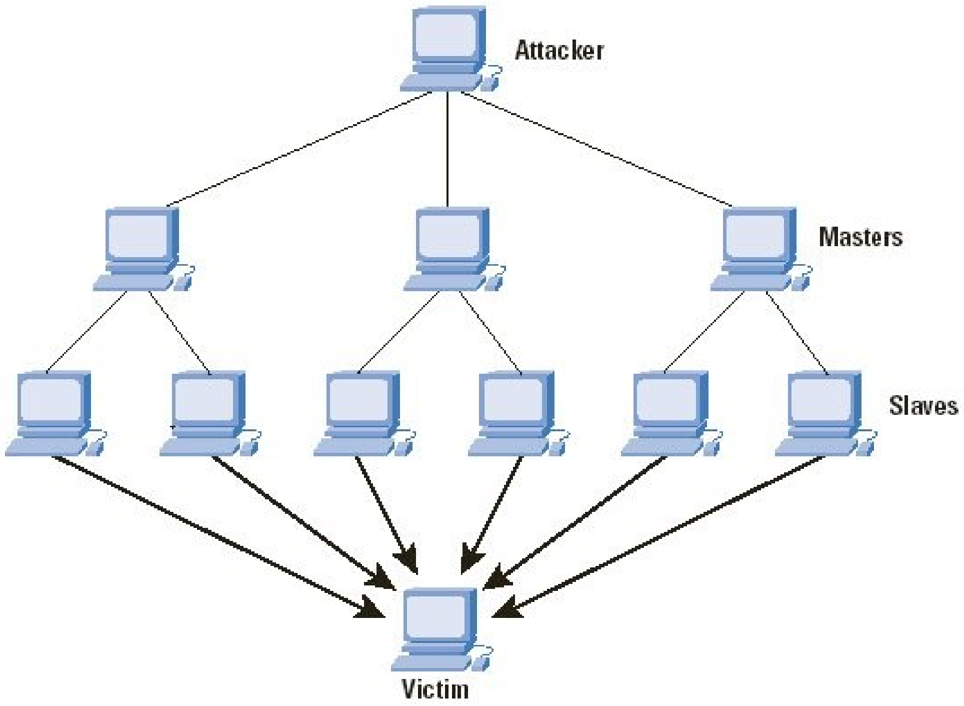
5 Browser sends session cookies to the perpetrator, enabling access to the victim's private data

https://www.incapsula.com/web-application-security/reflected-xss-attacks.html

Denial of Service (DoS)

- Web browser impersonator
- DDoS Bots
- Single Vector attack
- Large scale DDoS attack
- Multi Vector attack
- DDoS Trojan
- Local File Inclusion
- SQL Injection
- Anonymization service (Proxy/VPN)

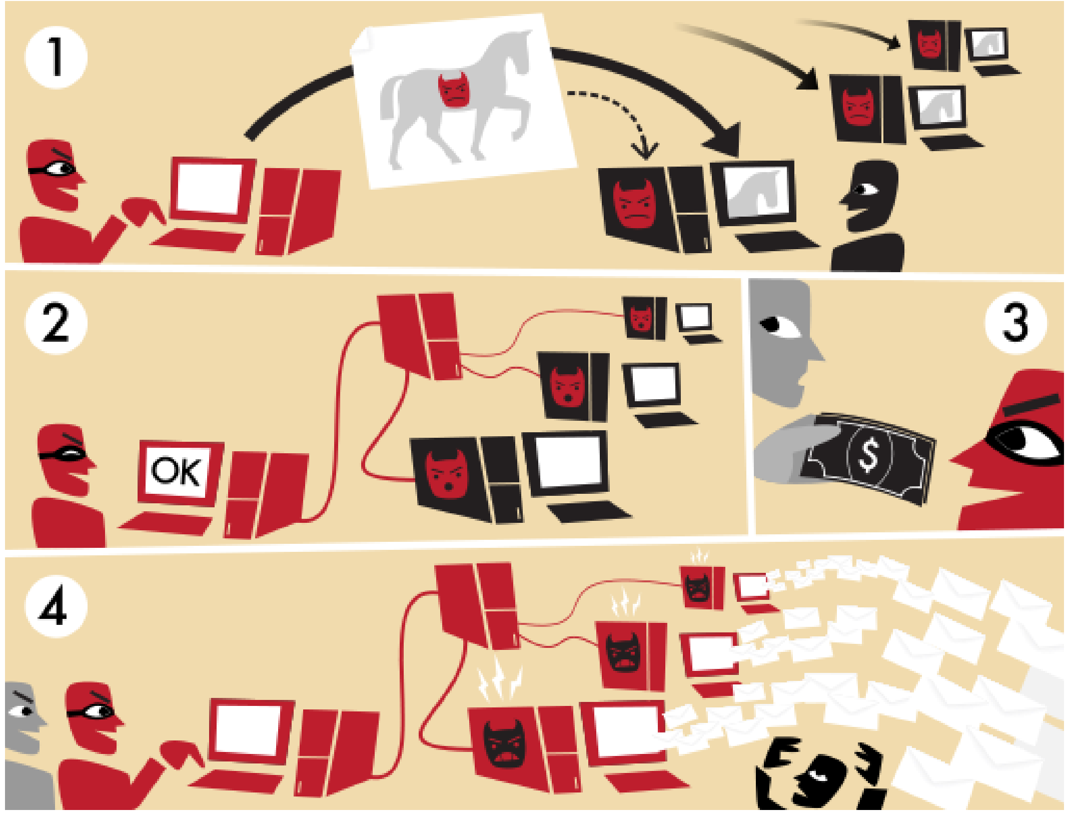
- Network layer attack
- Application layer attack
- Virus Infection
- Malware Activation
- Network compromise
- Loss of customer trust
- Data Theft
- Spam
- Phishing



http://linuxaria.com/article/mitigating-ddos-attacks

Botnet

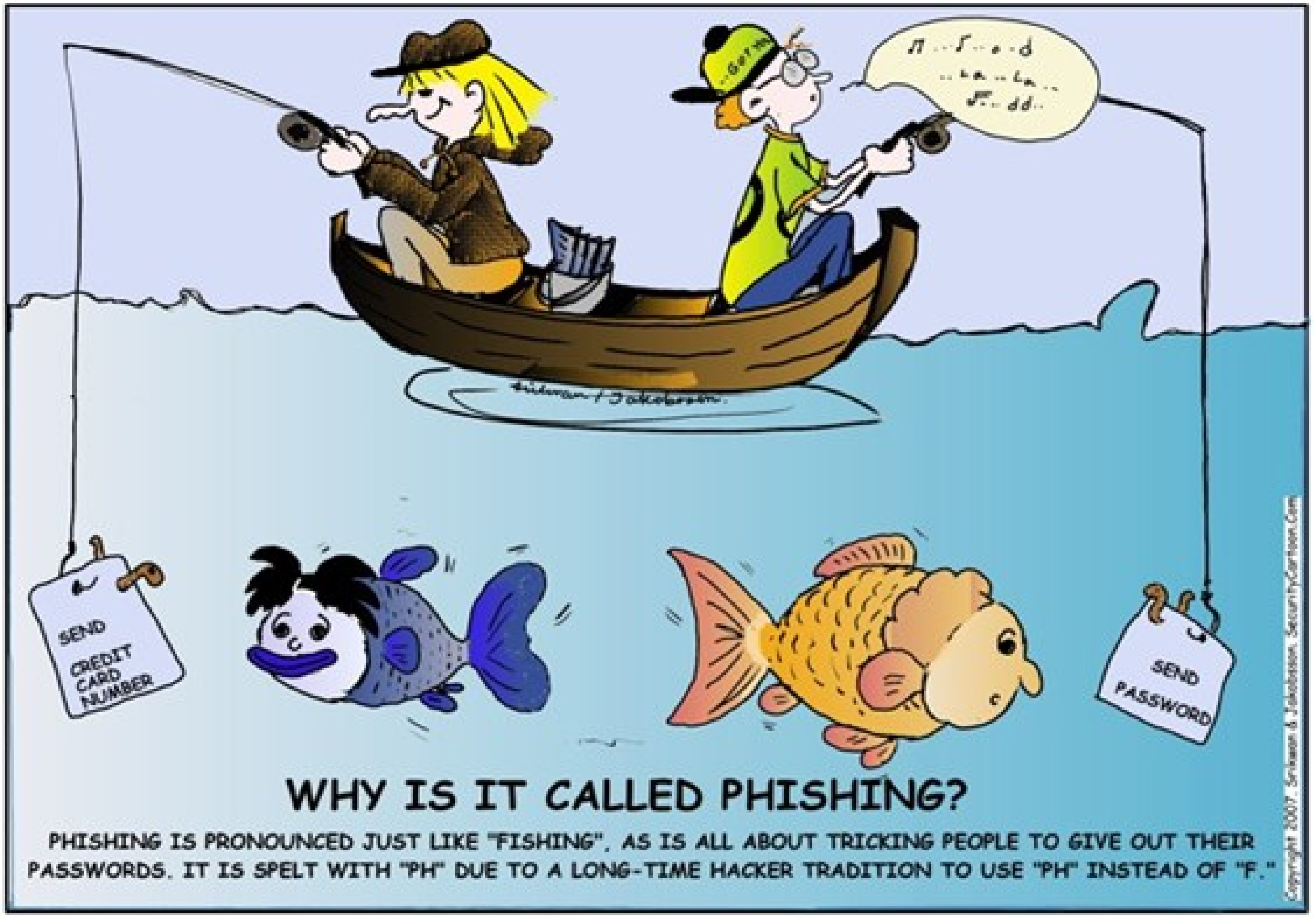
- Command and Conquer bots
- Spam bots
- Malware bots
- IoT bots
- Bots for DDoS
- Ad-Fraud botnet
- Multitenant bot
- Ramnit
- Nectus botnet
- DDoS as a Service



https://en.wikipedia.org/wiki/File:Botnet.svg

Phishing

- Ransomware
- CEO Fraud
- Fake Emails
- Water-holing
- Spear phishing



WHY IS IT CALLED PHISHING?

PHISHING IS PRONOUNCED JUST LIKE "FISHING", AS IS ALL ABOUT TRICKING PEOPLE TO GIVE OUT THEIR PASSWORDS. IT IS SPELT WITH "PH" DUE TO A LONG-TIME HACKER TRADITION TO USE "PH" INSTEAD OF "F."

http://biodataofdrvhp.blogspot.my/2013/02/what-is-phishing.html

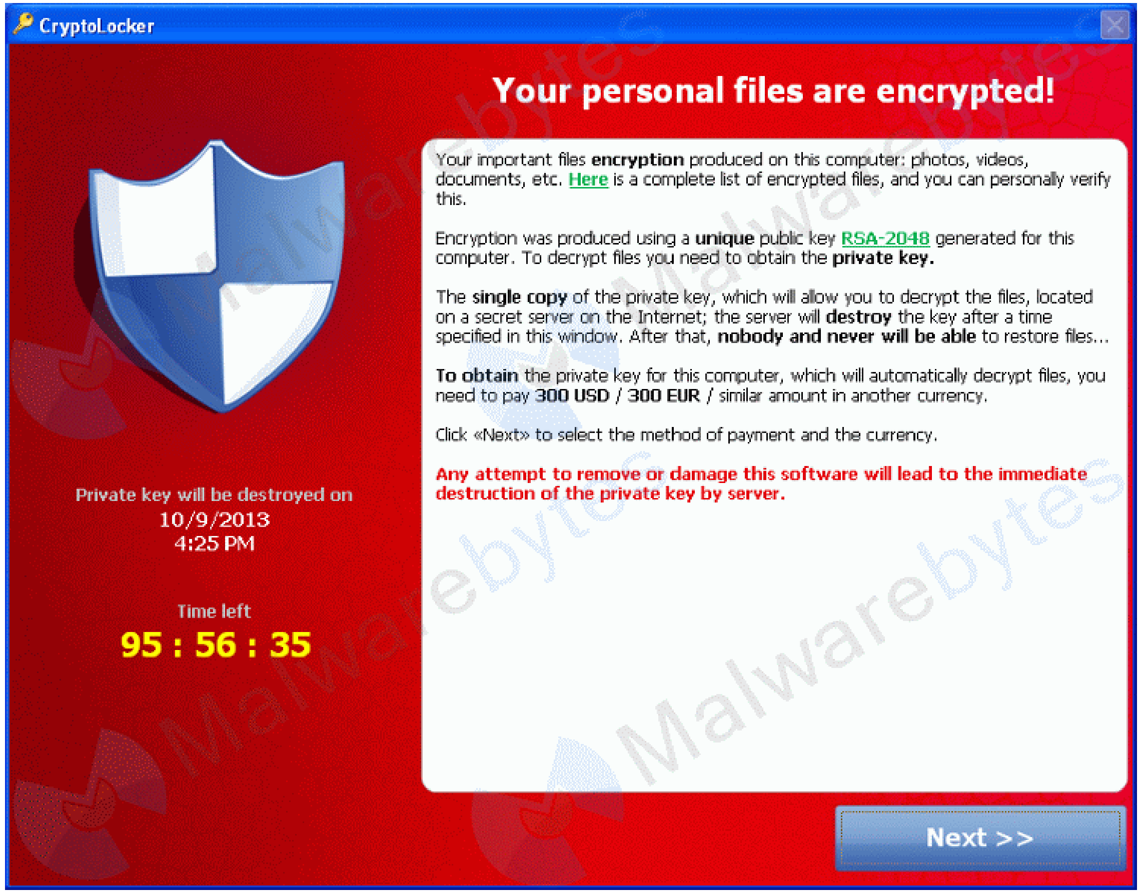
Spam

- Malware
- Malicious URL
- Phishing
- Spam botnets
- Vulnerability scanning
- Obfuscating of messages
- Fake orders/bills/Notifications
- Ransomware Trojans
- “Snowshoe” spam
- Spam URL

http://www.antispam.br/conceito/

Ransomware

- Spam botnet
- Exploit kits
- Drive by downloads
- Infected USBs
- Encryption of infected computers
- Ransomware as a Service



Your personal files are encrypted!

Private key will be destroyed on
10/9/2013
4:25 PM

Time left
95 : 56 : 35

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

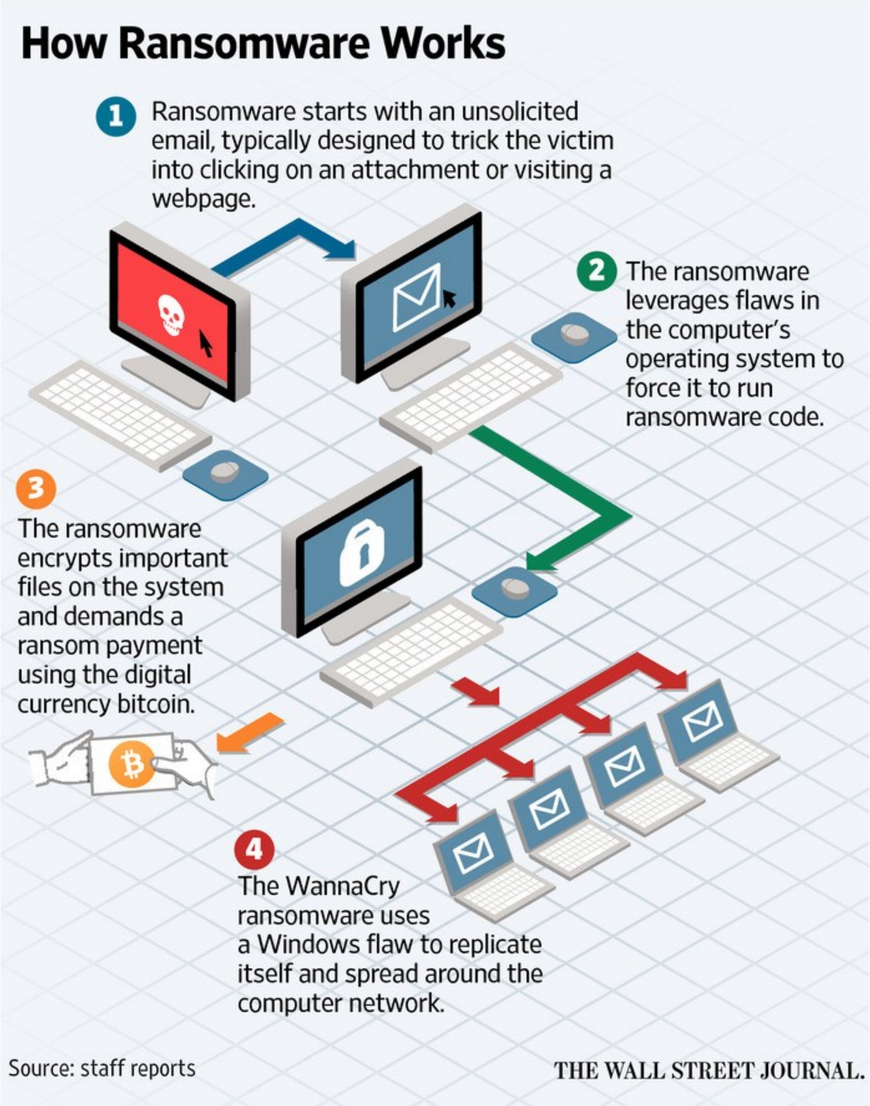
To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD** / **300 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

http://www.zonavirus.com/noticias/2015/proteccion-contra-los-ransomware.asp

How does Ransomware work?



How Ransomware Works

1. Ransomware starts with an unsolicited email, typically designed to trick the victim into clicking on an attachment or visiting a webpage.

2. The ransomware leverages flaws in the computer's operating system to force it to run ransomware code.

3. The ransomware encrypts important files on the system and demands a ransom payment using the digital currency bitcoin.

4. The WannaCry ransomware uses a Windows flaw to replicate itself and spread around the computer network.

Source: staff reports

THE WALL STREET JOURNAL.

Insider threat

- Privilege abuse
- Data mishandling
- Use of non-approved hardware
- Use of inappropriate software
- Abuse of privilege possession
- Espionage
- Fraud
- Monetization
- Sabotage
- Intellectual Property theft

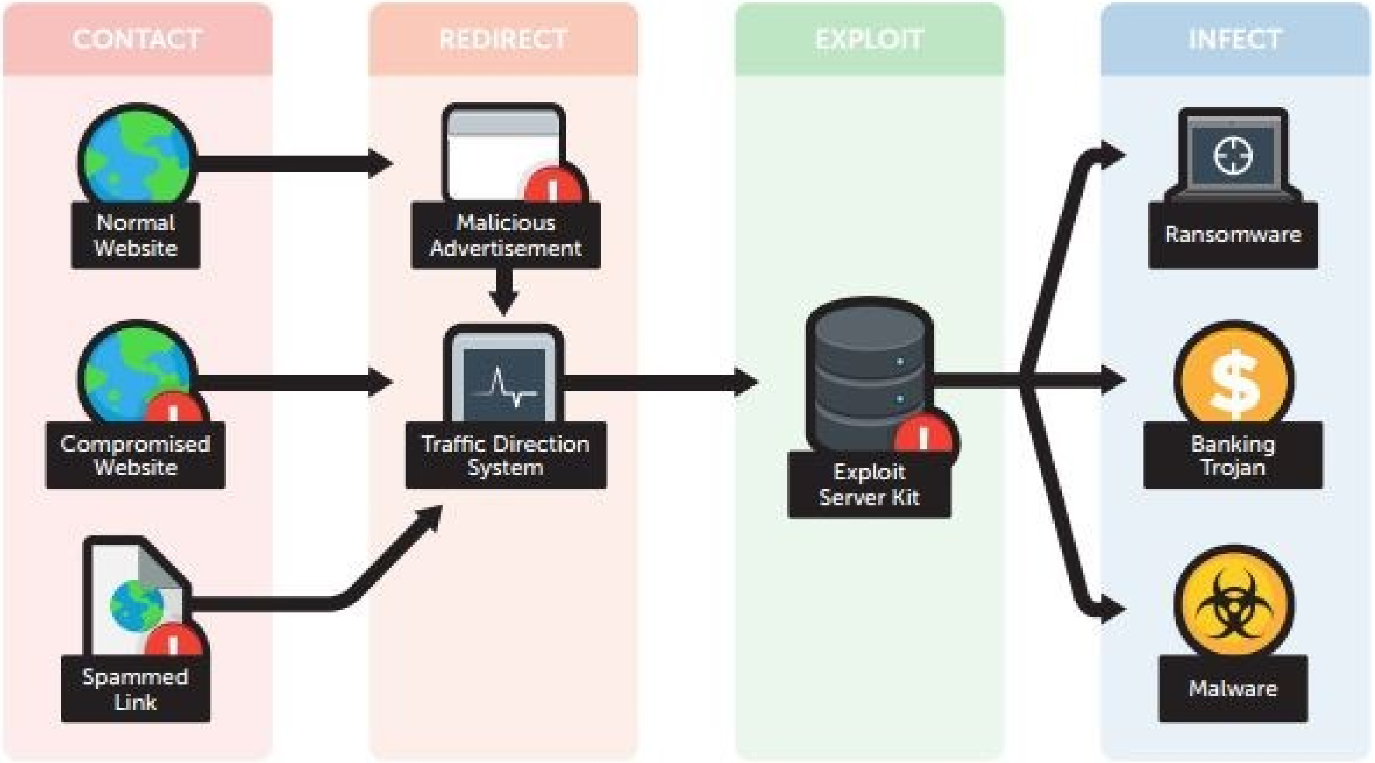
https://erick.rudiak.com/ciso/all-threats-are-insider-threats/

Physical damage/theft/loss

- Data breaches
- Information theft
- Weak encryption of storage media
- Uncontrolled physical access
- ATM fraud
- Physical media – laptop, USB drives, mobile phones, CD/DVDs, Webcam

Exploit Kits

- Malware installation
- Domain shadowing
- Ransomware
- Click Fraud
- Malware distribution
- Exploit kit as a Service



https://www.techeconomy.it/2015/09/22/abc-sicurezza-exploit-kit/

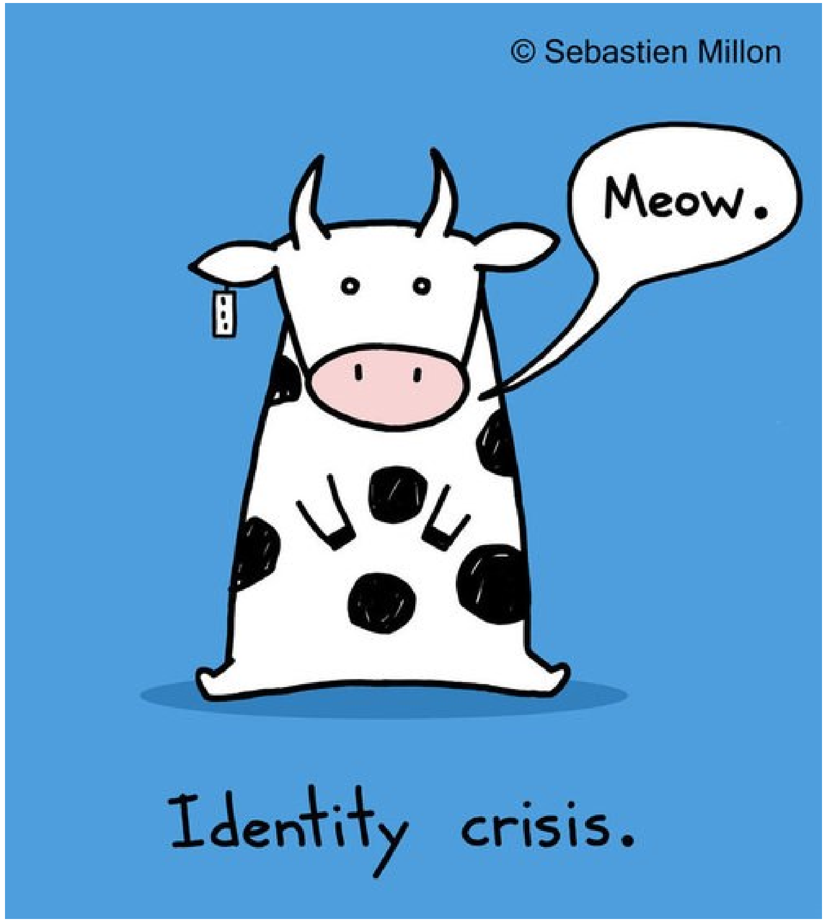
Data Breaches

- Stolen credentials
- Brute force attacks
- Phishing attacks
- Poor data protection
- Malware
- Backdoors
- Phishing
- Identity Theft
- Theft/Loss
- Insider threat
- Information Leakage
- Malware
- Web-based attacks

http://www.ashimmy.com/identity_theft/

Identity theft

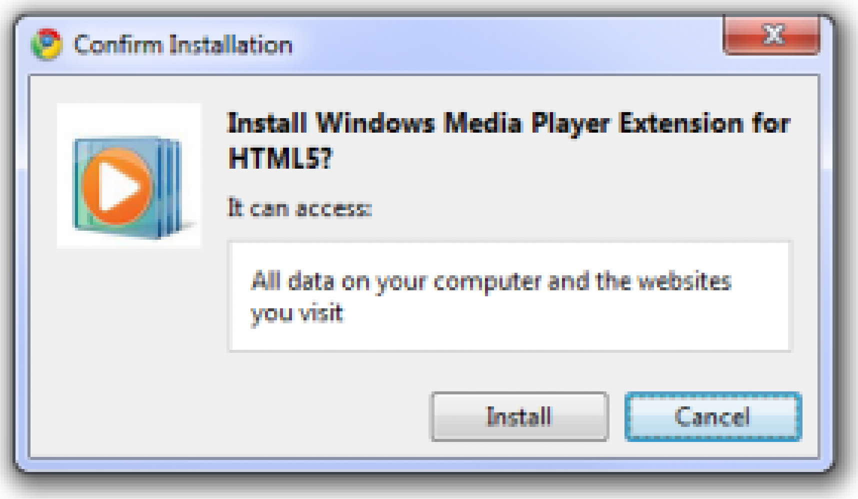
- Stolen credentials
- Brute force attacks
- Phishing attacks
- Malware
- Backdoors
- Phishing
- Identity Theft
- Theft/Loss
- Insider threat
- Information Leakage
- Malware
- Web-based attacks
- Fraud and Scams
- Botnets



http://yukaichou.com/gamification-study/identity-consistency-forces-ownership-possession/

Information Leakage

- Weakness in runtime systems
- Misconfiguration
- Programming errors
- User behaviour
- Unencrypted/weak encrypted user data
- Fake applications
- Fake offerings
- Web-based attacks
- Browser vulnerabilities
- Network communication vulnerabilities
- Mobile Application leaks
- Virtual currency vulnerabilities
- Fraud and Scams



Install Windows Media Player Extension for HTML5?

It can access:

All data on your computer and the websites you visit

https://pureinfotech.com/how-to-enable-webm-video-codecs-for-internet-explorer-9/

Cyber Espionage

- Advanced Persistent Threat (APT)
- Phishing
- Malware
- Spying tools/Cyber weapons
- Surveillance/Interception tools
- Zero-day vulnerabilities

ALLIED PRODUCTION
ALLIED MILITARY PLANS
BUT HEINRICH X*C!!!* VE GOT TO KNOW!
WHAT THEY DON'T KNOW WON'T HURT US!
KEEP YOUR EYES OPEN AND YOUR MOUTH SHUT!

https://commons.wikimedia.org/wiki/File:%22WHAT_THEY_DON'T_KNOW_WON'T_HURT_US%22_-_NARA_-_516132.jpg

What is a CIRT?

- A team that responds to cybersecurity incidents
- Provide services to a defined constituency
- Assist in effectively identifying a threat, coordinate at national level and regional levels
- Information dissemination
- Act as a focal point for the constituency

Need for National CIRT

YOUR CIRT

- Serve as a trusted focal point
- Develop a capability to support incident reporting.
- Develop an infrastructure for coordinating response.
- Conduct incident, vulnerability & Artifact analysis.
- Participate in cyber watch functions.
- Help organizations develop their own incident management capabilities.
- Provide language translation services.
- Make security best practices & guidance available.
- Provide awareness, education & trainings

Functions and Requirements

What does a CIRT do?

- Provides a single point for reporting incidents
- Assists the organizational constituency and general computing community in preventing and handling computer security incidents
- Share information and lesson learned with other CIRT / response teams and appropriate organizations and sites.

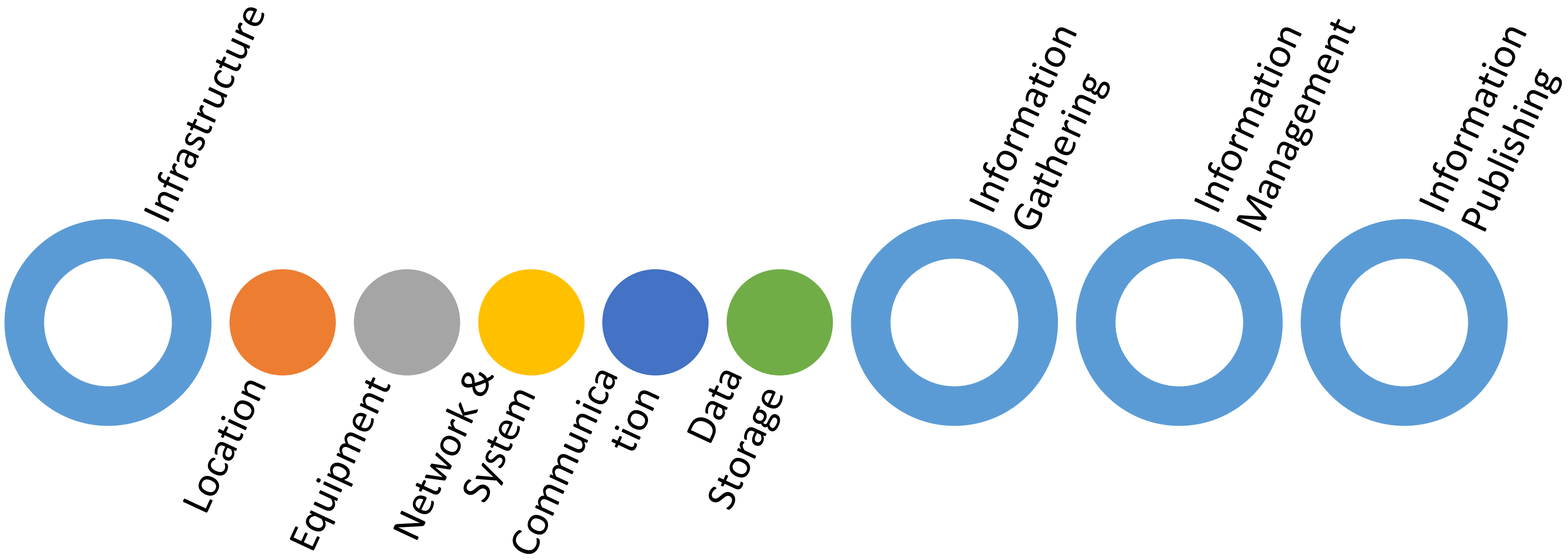
CIRT Framework

National CIRTs drive and promote:

- National Cybersecurity Strategies/Policies
- Cyber Forensics services
- Governance/Legislations
- Critical National Information Protection
- Training and Awareness
- Research
- International Cooperation
- Security Assurance

Functions and Requirements

CIRT relies on a number of mechanisms for its operations. Some of them being:



Functions and Requirements

Baseline capabilities

- Define minimum set of CIRT capabilities that address the priorities and challenges of a National CIRT

Mandate & Strategy

- Need a clear mandate to serve the constituency
- Their roles should be part of the National Cybersecurity strategy, establish with a body with adequate funding

Service Portfolio

- CIRT services should be clearly defined with its mandate and strategy
- Reduce the vulnerabilities of its critical sectors to cyber attacks and provide responses when attacks occur

Operation

- Must be able to respond to incident cross border since incidents happens on a global scale
- Must be highly capable and competent to ensure operational effectiveness

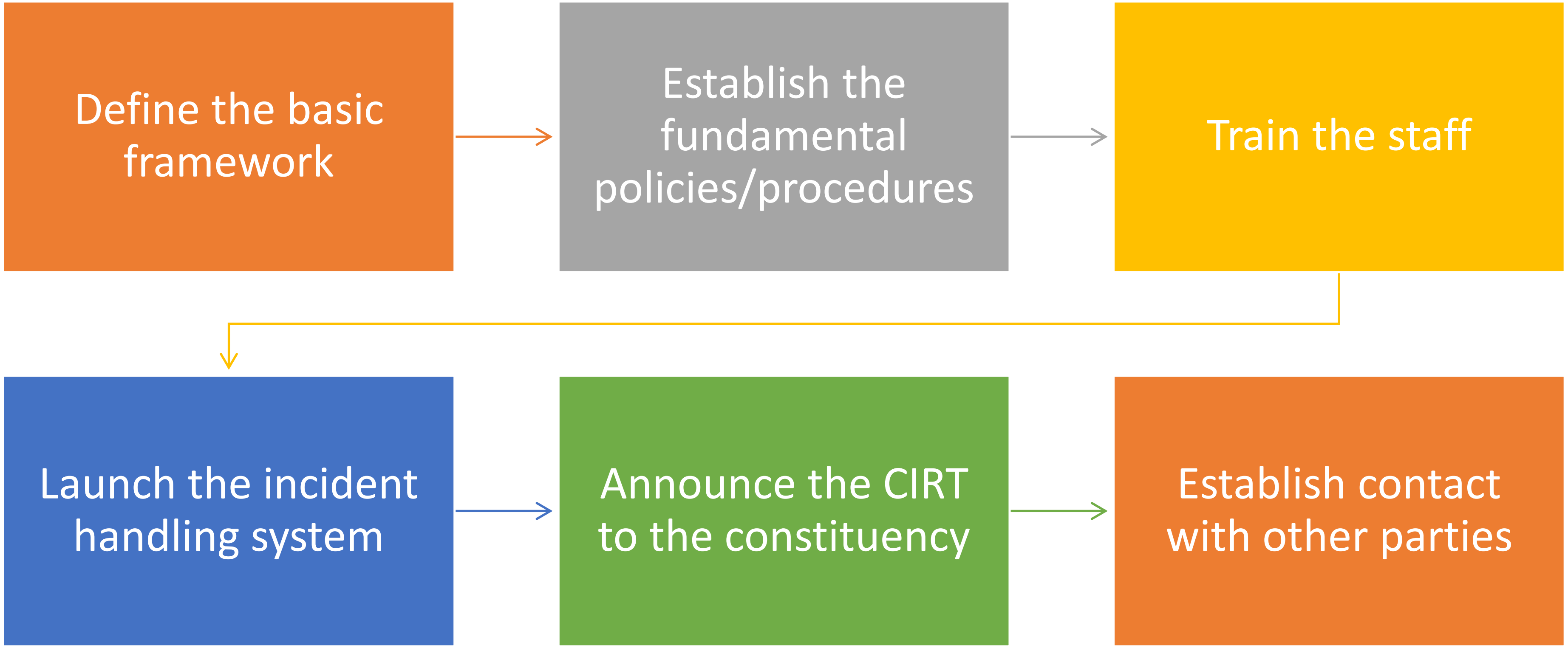
Cooperation

- Effective cooperation between all CIRT at all levels required
- Establish trust relationship between bodies
- Effective in building relationships

CIRT Services

Reactive Services	Proactive Services	Artifact Handling
Alerts & Warnings	Announcements	Artifact Analysis
Incident Handling	Technology Watch	Artifact response
Incident Analysis	Security Audits	Artifact response coordination
Incident response support	Security Assessments	**Security Quality Management**
Incident response coordination	Configuration & Maintenance of Security	Risk Analysis
Incident response on site	Development of Security Tools	BC and Disaster Management
Vulnerability Handling	Intrusion detection services	Security Consulting
Vulnerability Analysis	Security related information dissemination	Awareness Building
Vulnerability Response		Education/Training
Vulnerability Response Coordination		Project Evaluation or Certification

Creating a CIRT : High level approach



Define the basic framework

Establish the fundamental policies/procedures

Train the staff

Launch the incident handling system

Announce the CIRT to the constituency

Establish contact with other parties

Collaboration among CIRTs

- CIRT have to inter-operate to get their job done
- Consider joining the regional / global community (FIRST)
- FIRST: Forum of Incident Response and Security Teams
  - Foster coordination in incident prevention, detection and response
  - Strives for excellence and improvement to ensure integrity, quality, performance and mutual respect among other CIRTs
  - Provides a trusted mechanism to share sensitive incident information amongst response teams

Improving Security Together

ITU : I Thank U

CELEBRATING 25 YEARS OF ACHIEVEMENTS