Seminario della 67/ Sessione dell 'Istituto Alti Studi per la Difesa "Sfide globali«/Ministero della Difesa
14 gennaio 2016

"Cyberthreat e Cybersecurity: tutto ciò che un decisore deve necessariamente sapere "

Elisabetta ZUANELLI
Università degli Studi di Roma "Tor Vergata"
CReSEC (Centro di Ricerca e sviluppo sull'E-Content)

Il percorso

1. il cyberspazio e le nuove tecnologie
2. definizioni
3. gli attanti
3. le vittime degli attacchi, le fonti e le tecnologie
4. rapporti e tendenze
5. la risposta istituzionale UE e USA
6. le infrastrutture critiche
8. la percezione e la previsione
9. i nodi
10. le soluzioni

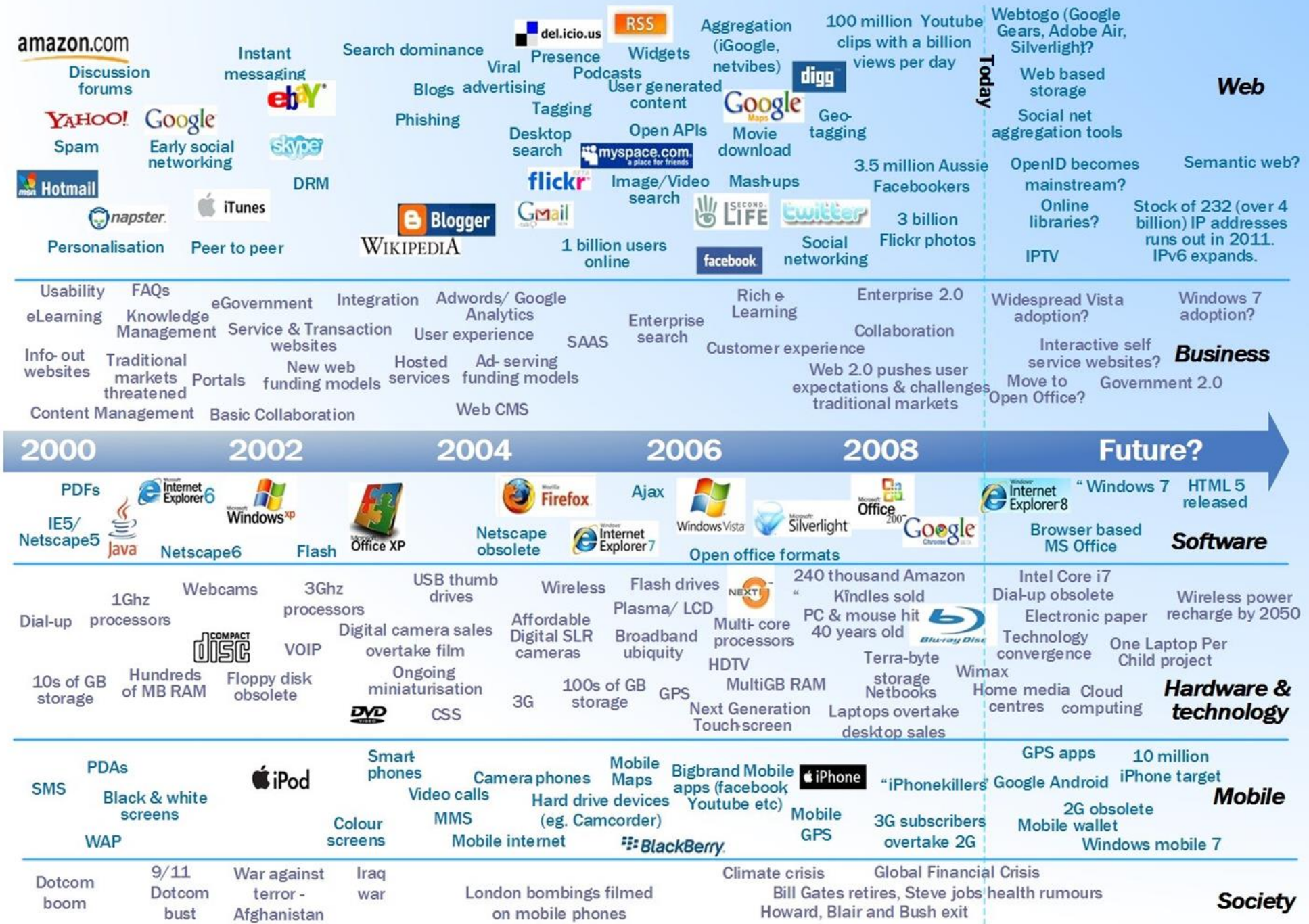
Il cyberspazio e le nuove tecnologie

La rivoluzione del micromillennio: sicurezza nelle Reti, piattaforme e servizi online

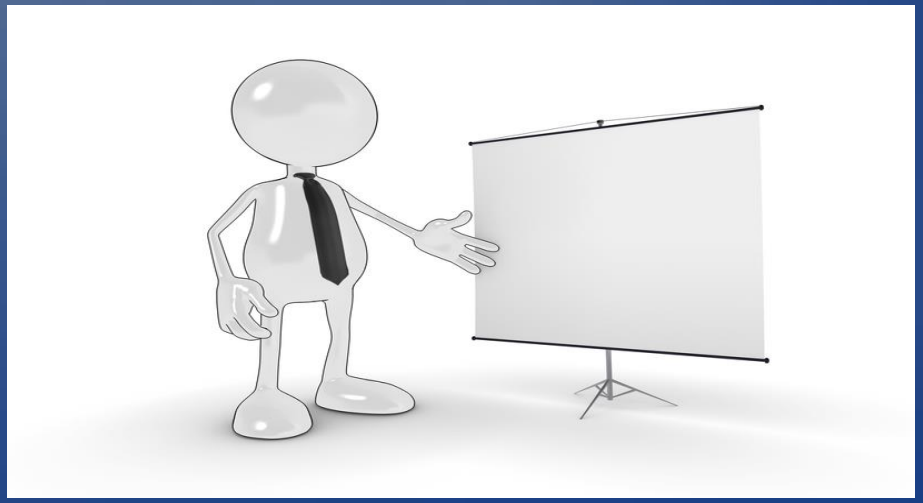
le interazioni e le transazioni on line e la gestione remota:

- piattaforme e nuovi servizi on line: i *player* mondiali/GAFTAM
- le infrastrutture critiche
- i social network
- le app per mobile
- il cloud
- l'IoT e l'IoE
- l'Industry 4.0

Vecchie e nuove tecnologie



Definizioni



Il cyberspace

Il **cyberspazio** è un insieme di infrastrutture informatiche interconnesse che comprende *hardware*, *software*, dati e utenti così come le relazioni logiche tra questi.

Include, tra le altre cose, Internet, le reti di comunicazioni, i sistemi attuatori di processi e i dispositivi mobili forniti di una connessione di rete

La cybersecurity

La **sicurezza informatica** è la condizione in cui il ciberspazio è protetto, rispett

La cyberthreat

http://itlaw.wikia.com/wiki/Cyber_threat

Cyber threat(s)

." È una qualsiasi azione forzosa identificata, diretta verso l'accesso, l'esfiltrazione, la manipolazione o la compromissione dell' integrità , della riservatezza, della sicurezza o la disponibilità di dati, di un'applicazione o di un sistema federale, senza l'autorizzazione necessaria . "

." Sono potenziali eventi cibernetici che potrebbero causare risultati indesiderati , con conseguente danno a un sistema od organizzazione. Le minacce possono provenire esternamente o internamente e da individui od organizzazioni .”

Il triangolo concettuale

cybersecurity

cyberthreat

violazioni/attacchi cibernetici

Gli attanti


DEFINE
MEASURE
ANALYZE
IMPROVE
CONTROL
Improvement Process
gg65543733 www.gograph.com

I ruoli

le vittime:

- i singoli
- le istituzioni pubbliche e private
- le aziende
- i governi
- i gruppi politici e religiosi

- **gli attaccanti:**
- i governi
- l'economia del cybercrime
- i committenti
- gli hacker

attaccanti

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	Variazioni 2012 su 2011	Variazioni 2013 su 2012	Variazioni 2014 su 2013	Variazioni 2014 su 2011	Trend 2015
Cybercrime	170	633	609	525	272,35%	-3,79%	-13,79%	208,82%	
Hacktivism	114	368	451	236	222,81%	22,55%	-47,67%	107,02%	
Espionage	23	29	67	69	26,09%	131,03%	2,99%	200,00%	
Information Warfare	14	43	25	42	207,14%	-41,86%	68,00%	200,00%	
© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia									

vittime

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	Variazioni 2012 su 2011	Variazioni 2013 su 2012	Variazioni 2014 su 2013	Variazioni 2014 su 2011	Trend 2015
Gov - Mil - LEAs - Intelligence	153	374	402	211	144,44%	7,49%	-47,51%	37,91%	→
Others	97	194	146	173	100,00%	-24,74%	18,49%	78,35%	↑
Entertainment / News	76	175	147	77	130,26%	-16,00%	-47,62%	1,32%	→
Online Services / Cloud	15	136	114	103	806,67%	-16,18%	-9,65%	586,67%	↑
Research - Education	26	104	70	54	300,00%	-32,69%	-22,86%	107,69%	↑
Banking / Finance	17	59	108	50	247,06%	83,05%	-53,70%	194,12%	↑
Software / Hardware Vendor	27	59	46	44	118,52%	-22,03%	-4,35%	62,96%	→
Telco	11	19	19	18	72,73%	0,00%	-5,26%	63,64%	→
Gov. Contractors / Consulting	18	15	2	13	-16,67%	-86,67%	550,00%	-27,78%	↓
Security Industry	17	14	6	2	-17,65%	-57,14%	-66,67%	-88,24%	↓
Religion	0	14	7	7	-	-50,00%	0,00%	-	→
Health	10	11	11	32	10,00%	0,00%	190,91%	220,00%	↑
Chemical / Medical	2	9	1	5	350,00%	-88,89%	400,00%	150,00%	↑
Critical Infrastructures	-	-	37	13	-	-	-64,86%	-	→
Automotive	-	-	17	3	-	-	-82,35%	-	→
Organizations / ONG	-	-	19	47	-	-	147,37%	-	↑
GDO / Retail	-	-	-	20	-	-	-	-	↑

Le minacce

- modalità
- tecnologie
- impatto

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtuali-sation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2014[1]

Minacce e impatto

Chiarezza concettuale:

tipi di attacchi/tecnologie **tipi di effetti**

malicious code

web based attacks

web application attacks

botnets

spam, phishing

exploit kits

denial of service

data breaches

physical damage/theft/loss

information leakage

identity theft/fraud

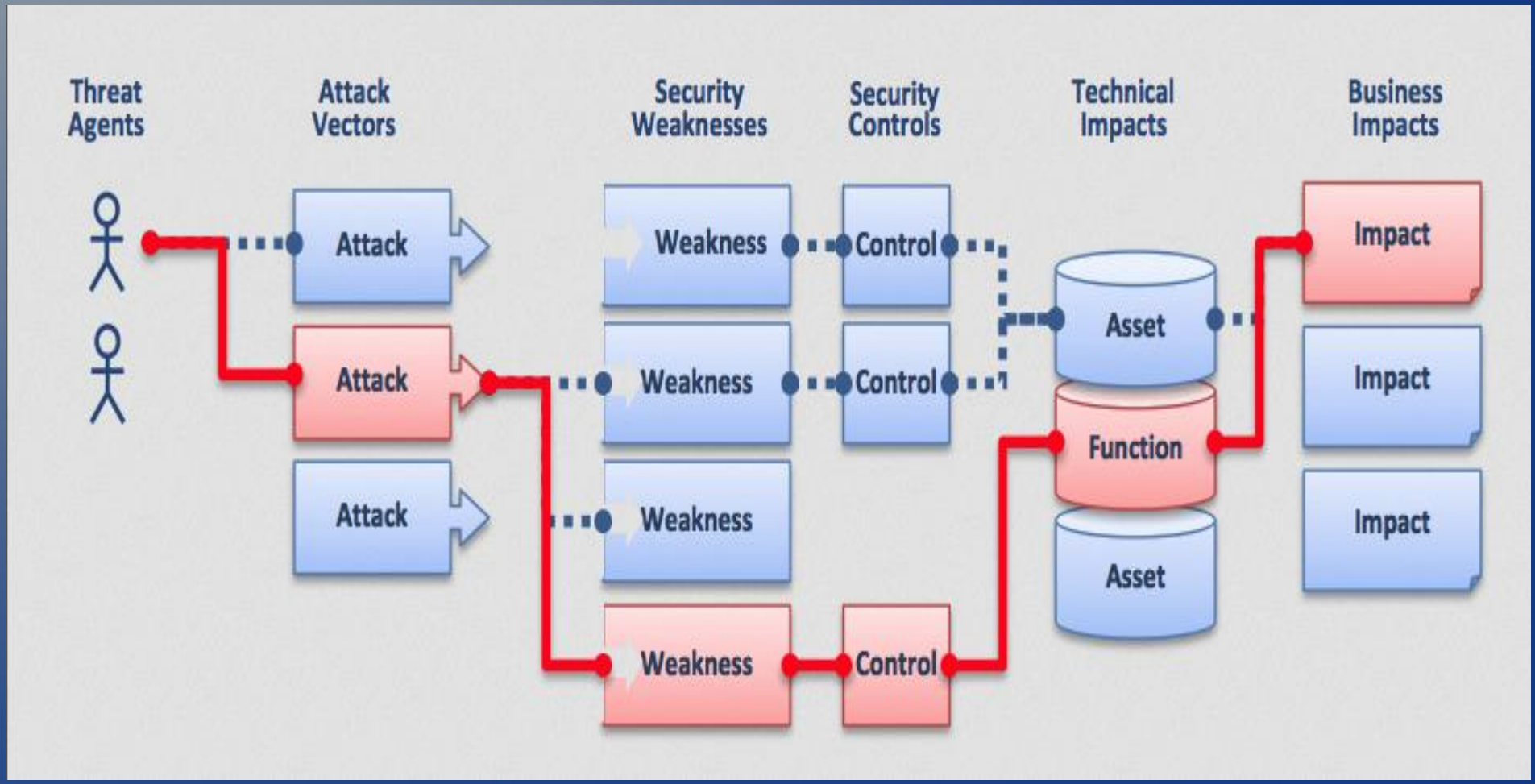
cyber espionage

Tecnologie oggetto d'attacco

- cyber physical systems e CIP
- mobile computing
- cloud computing
- trust infrastructures
- Big data
- IoT
- netw. virtualisation

L'impatto
Impact

http://www.owasp.org/index.php/File:2010-T10-ArchitectureDiagram.pngNeil Smithline -



La risposta di sistema

La risposta: il mercato, gli stakeholder e i venditori di sicurezza

The global Cyber Security market size is estimated to grow from $106.32 Billion in 2015 to $170.21 Billion by 2020, at a Compound Annual Growth Rate (CAGR) of 9.8%

Stakeholders:

Cyber security vendors

Networking solution providers

Independent Software Vendors (ISVs)

Software vendors

System integrators

Value-added resellers

Service providers and distributors

Research organizations

IT security agencies

Suppliers, distributors, and contractors

Consulting companies

Cloud Business Intelligence (BI) platform vendors/cloud infrastructure providers

Investors and venture capitalists

I submarket

Security Types:

- Network security
- Endpoint security
- Application security
- Content security
- Wireless security
- Cloud security

By Service:

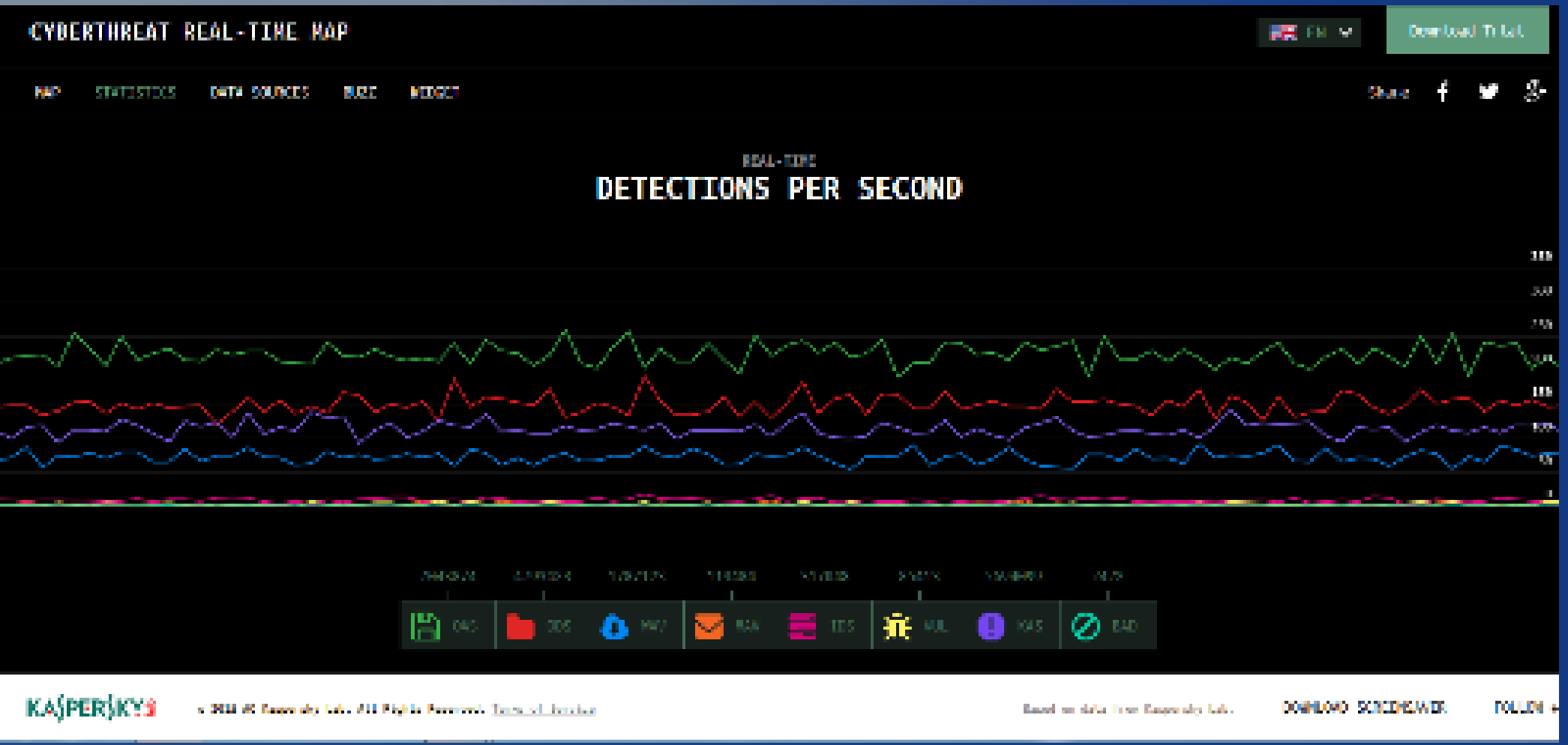
- Consulting
- Design and integration
- Risk and threat assessment
- Managed security services
- Training and education

By Vertical:

- Aerospace, defense, and intelligence
- Government (excluding defense) and public utilities
- Banking, Financial Services, and Insurance (BFSI)
- Telecommunication
- Healthcare
- Retail
- Manufacturing

Data: statistics Kaspersky

OAS On Access Scan-WAS Web Access Antivirus-MAV Mail Antivirus-IDS Intrusion Detection Scan-VS VulnerabilityScan-KAS Kaspersky Anti-Spam-BAD Botnet Activity Detection



soluzioni

- Tecnologiche
- Manageriali/organizzative
- Comportamentali
- R&D
- Training

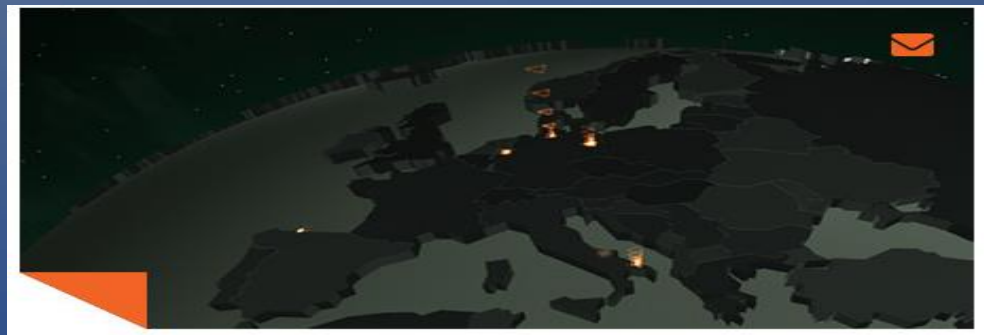
Data sources Kaspersky

IDS

IDS (Intrusion Detection System) shows network attacks detection flow.

KAS

KAS (Kaspersky Anti-Spam) shows suspicious and unwanted email traffic discovered by Kaspersky Lab's Reputation Filtering technology.



MAV

MAV (Mail Anti-Virus) shows malware detection flow during Mail Anti-Virus scan when new objects appear in an email application (Outlook, The Bat, Thunderbird). The MAV scans incoming messages and calls OAS when saving attachments to a disk.

BAD

BAD (Botnet Activity Detection) shows statistics on identified IP-addresses of DDoS-attacks victims and botnet C&C servers. These statistics were acquired with the help of the DDoS Intelligence system (part of the solution Kaspersky DDoS Protection) and is limited to the data on botnets that were detected and analyzed by Kaspersky Lab.

Il rapporto Symantec Norton 2015

il rapporto Symantec Norton 2015

At a Glance

- *More state-sponsored cyberespionage came to light in 2014.*
- *Attackers are using increasingly well-crafted malware that displays sophisticated software engineering and professionalism.*
- *Campaigns such as Dragonfly, Waterbug, and Turla infiltrated industrial systems, embassies, and other sensitive targets.*
- *The number of spear-phishing campaigns increased by 8 percent in 2014, while the number of daily attacks decreased as attackers become more patient, lying in wait and crafting more subtle attacks boosted by longer-term reconnaissance.*

Il contesto geopolitico globale

North America

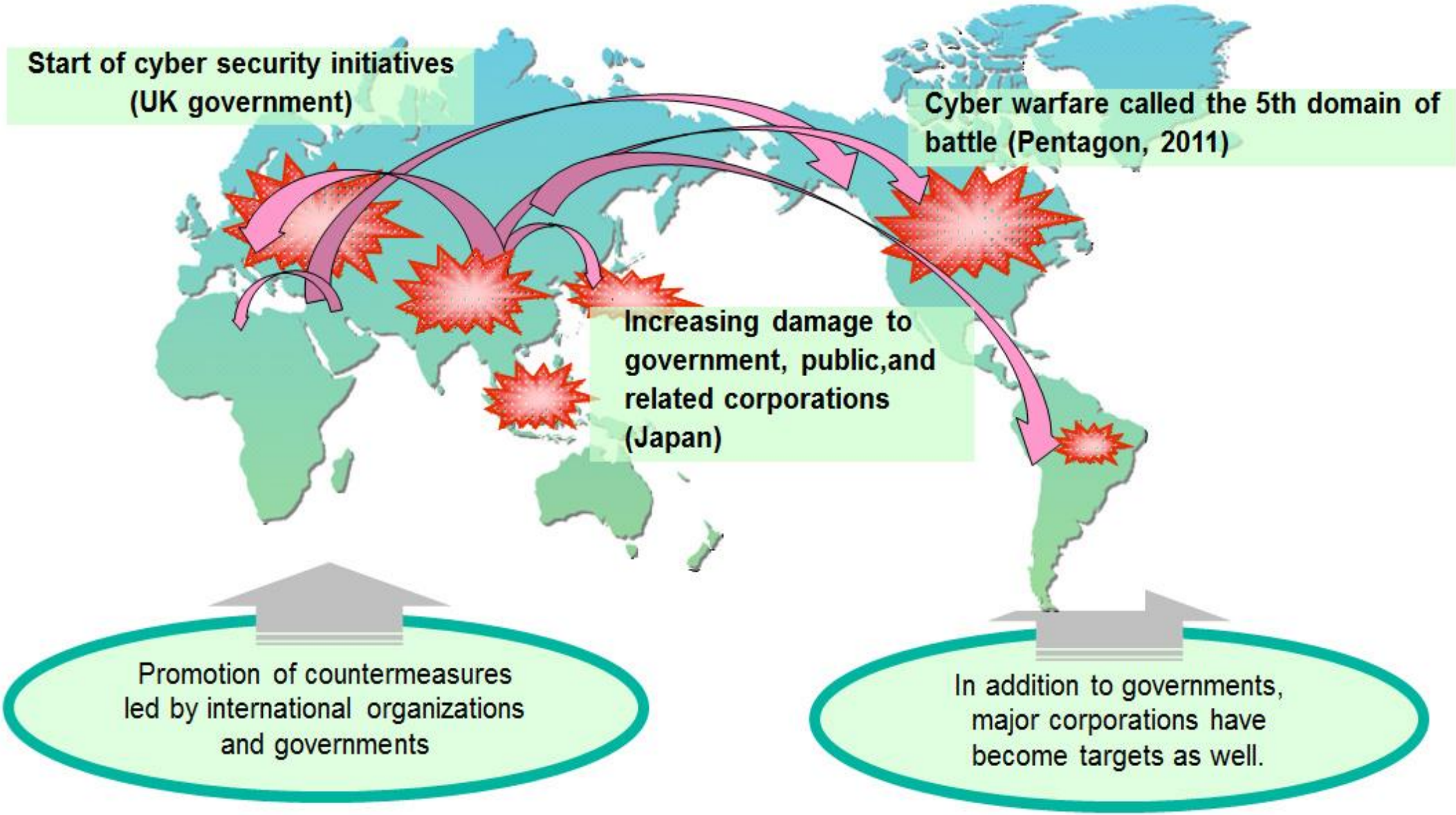
Europe

Asia-Pacific

Middle East and Africa

Latin America

Cybersecurity e cyberthreat: il geo-contesto globale



La risposta istituzionale

Le responsabilità istituzionali

USA

UE

stati membri

Italia

L'UE: EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive (2013)

1) Cybersecurity Strategy of the European Union: An Open, Safeand Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013

2) Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final - 7/2/2013 - EN

3) Executive Summary of the Impact Assessment - SWD(2013) 31 final - 7/2/2013

4) Impact Assessment - SWD(2013)32 final - 7/2/2013

Connessione azioni strategia digitale

Pillar III: Trust & Security

Action 28: Reinforced Network and Information Security Policy

Action 29: Combat cyber-attacks against information systems

Action 30: Establish a European cybercrime platform

Action 31: Analyse the usefulness of creating a European cybercrime centre

Action 32: Strengthen the fight against cybercrime and cyber-attacks at international level

Action 33: Support EU-wide cyber-security preparedness

Action 38: Member States to establish pan-European Computer Emergency Response Teams

Action 39: Member States to carry out cyber-attack simulations

Action 41: Member States to set up national alert platforms

L'Agenda sicurezza ENISA UE: vantaggi

The following table provides some examples inside the diversity of expected benefits and contributions to the EU businesses, citizens and the society in general for each of the commonalities identified above.

Topic / Benefits	Business	Citizens	Society
Fostering Assurance	Business will be able to operate across Digital Single Market (DSM) thanks to more uniform assurance/protection requirements and achieved levels.	Citizens will be able to compare offerings and make informed decisions based on cybersecurity assurance/protection levels.	Trust in digital space will increase.
Focussing on Data	Business will be able to build innovative data-driven services while being compliant with the data protection and privacy legislation.	Citizens will have means to monitor and enforce policies on data usage, as well as to express their preferences.	Wealth of data will be exploited for various purposes, from healthcare research to fraud detection.
Enabling secure execution	Business will save costs on security management and post-incident activities.	Citizens will enjoy higher level of protection while having more simplicity.	Integration and seamless move between life domains (e.g. work and home) will be achieved.
Preserving privacy	Less privacy breaches will lead to the increase of trust and will become competitive feature.	Citizens will have more guarantees that their privacy is respected.	Societal values will be preserved, such as respect of minorities, dignity, etc.
Increasing trust	Proportion of trust based on demonstrable trustworthiness will be increased.	Citizens will be enabled to make more informed decisions.	Society will evolve to trust digital institutions in a similar way to their trust in the physical world.
Managing cyber risks	More frequent and accurate assessment will lead to more effective use of resources.	Citizens will be able to make instant decisions based on risk "traffic light".	Notion of cybersecurity risk will become an essential part of digital culture.
Protecting the ICT infrastructure	Reduction of "out-of-business" due to ICT infrastructure downtimes and reduction of industrial espionage.	Availability of services that rely on ICT infrastructures.	Less disruptions in critical services for society.
Achieving User-centricity	More users, therefore potential customers, will access digital services.	Simplification will increase the use of advanced protection mechanisms.	Wellbeing achieved by citizens that feel comfortable with new or complex technologies.

Table 9. Example of expected benefits/contributions per research commonality

ENISA e NIS platform

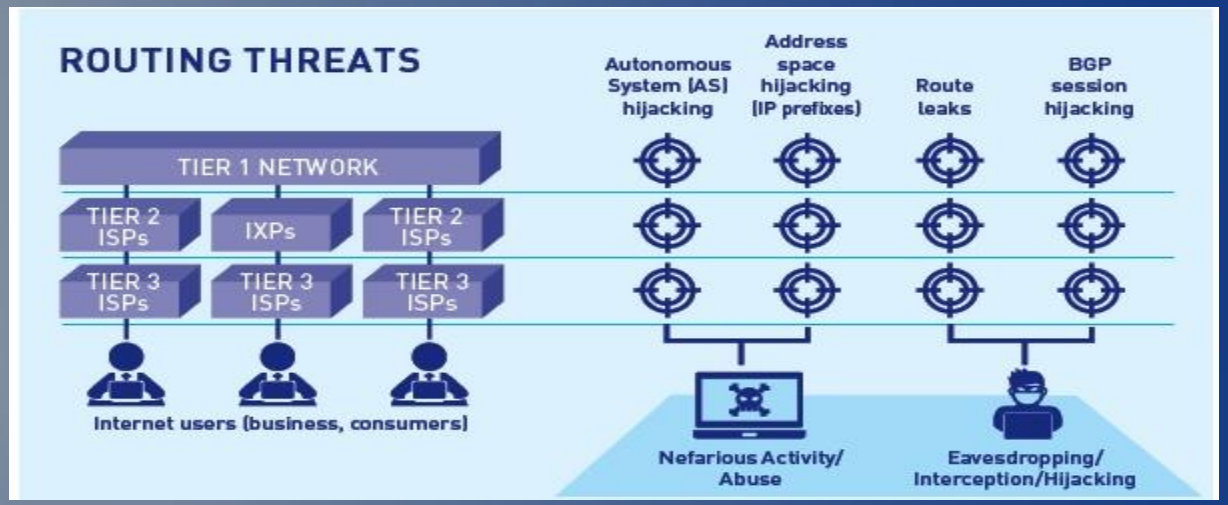
Project reference	Key research activities identified

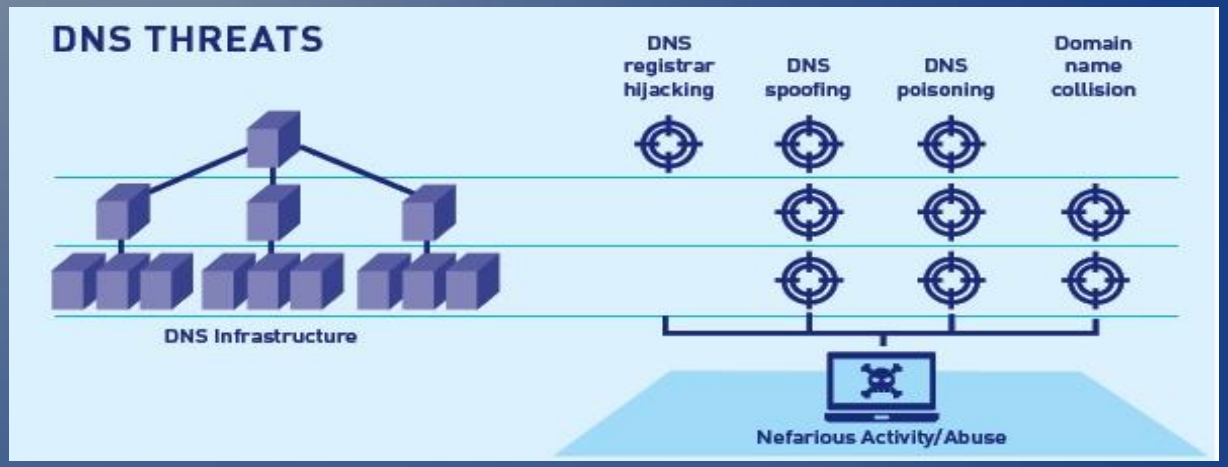
	– Security of Mobile Devices
	  ○ Mobile security is still in its infancy and all kind of security solutions are needed
	  ○ Confidentiality (privacy) and integrity seem to be the most important challenge to meet
	  ○ Evasion-resistant solutions, which potentially retrofit traditional malware need to be explored
	  ○ Exploring highly scalable technologies for efficient monitoring and analysis of security events that have the potential to compromise mobile devices
	– Legacy systems
	  ○ Exploration of a hybrid attack detection solution, which would marry BodyArmour to static protection approaches such as WIT
	  ○ How to evaluate the complexity of code fragments in existing binaries, so that one can focus the effective yet expensive symbolic execution on code that is more likely to have exploitable vulnerabilities
	– Usable security
	  ○ Usability guidelines for security researchers, a basic collection of do's and dont's for user interaction
	  ○ Usability of already existing security solutions.
	  ○ Incorporation of the usability decisions into the development process right from the beginning (raising awareness of people designing security solutions)
	– Botnets
	  ○ Exploring new ways to taking down botnets (e.g. alert users without becoming too intrusive, safe ways to penetrate people's computers and remove infections)
	  ○ Development of a legal framework for dealing with new, advanced botnets (e.g. how to take more invasive measures against resilient malicious infrastructures, how to strike back at machines that are located in other countries)
	– Malware
	  ○ Existing virus scanners and malware detectors cannot always keep up with malware variants that employ packing and polymorphism, need for more advanced malicious code scanning and analysis techniques
	  ○ Solutions based on runtime behavioural profiling and detection which are less prone to false alarms and have less runtime overhead than the existing solutions
	  ○ Process capacity of malware analysis systems (increased rate of new samples that must be analysed on a daily basis and the need for more complex analysis for non-trivial samples)
	– Social engineering and phishing
	  ○ Interdisciplinary research in two orthogonal dimensions: 1) effective methods for educating users about attacks, providing them with the basic skills for identifying them and 2) developing defence mechanisms for automatically identifying phishing attempts.
	  ○ Effective countermeasures for the ever increasing spear phishing attacks

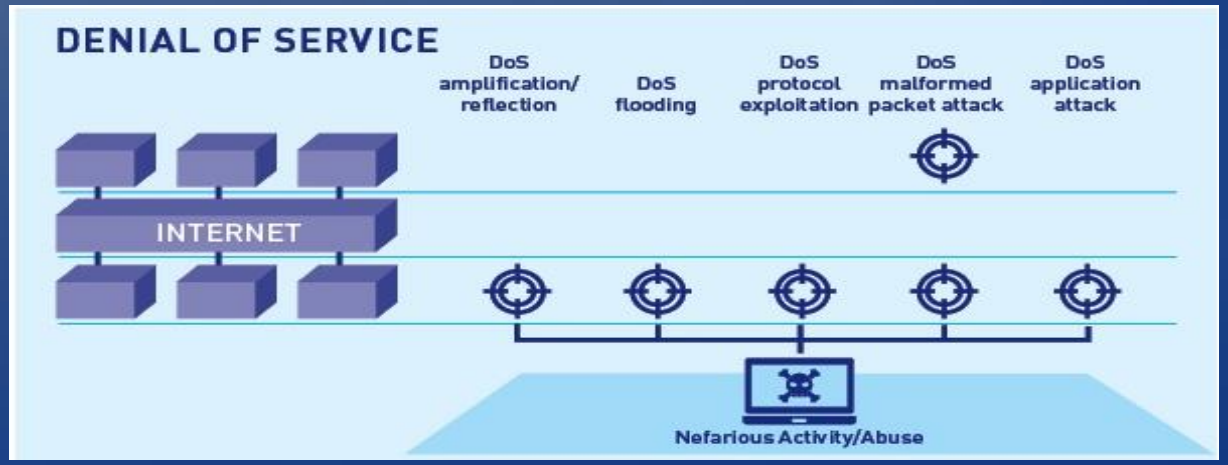
Project reference	Key research activities identified

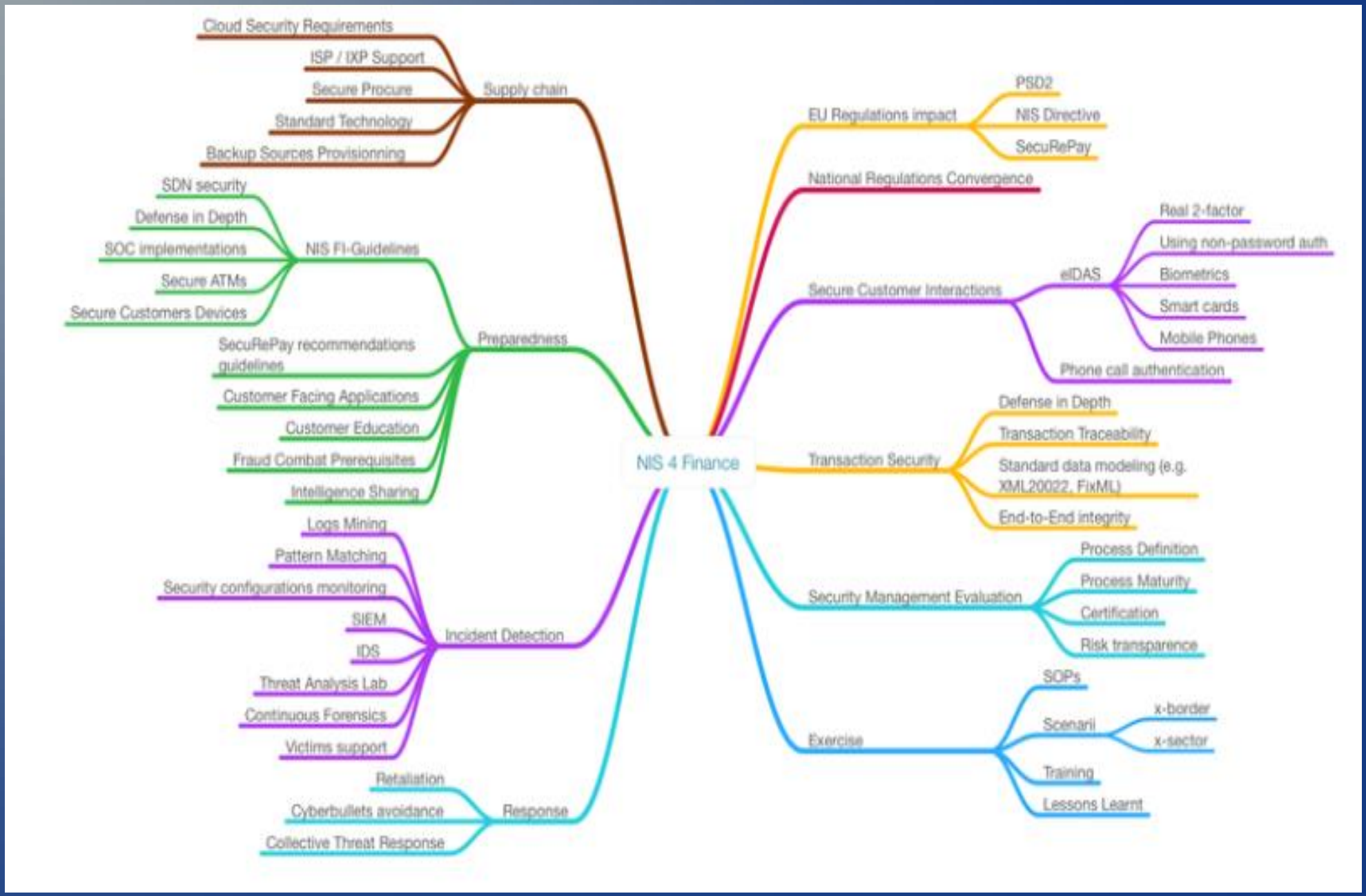
EFFECTPLUS	• Organisations
	  ○ Increase risk-awareness businesses
	  ○ Strengthening security measures businesses (tools for building secure systems, deploying suitable security metrics, security policies)
	  ○ Development of adequate certification and audit frameworks
	  ○ Cooperation on issues of national security, secure and trustworthy international data exchange system for tracking cyber threats/crimes
	• Authentication and authorization
	  ○ Developing biometrics that are ubiquitous but non-intrusive
	  ○ Achieving privacy, trust, identity management in mobile scenario's
	  ○ Developing a model of identity management to deal with digital vandals and cybercrime
	  ○ Global and secure individual authentication
	  ○ Development of universally acceptable digital identifiers
	• Could computing
	  ○ Developing cryptography for use in the cloud
	  ○ Enabling the use of trusted identity chains in the cloud
	  ○ Doing risk analysis in the could context
	  ○ Achieving control and enforcement across domains
	  ○ Security and privacy preservation for cloud applications and service infrastructures
	• Privacy
	  ○ Achieving transparency for the end user
	  ○ Developing the ability to permanently erase digital trails
	  ○ Privacy preserving data processing
	  ○ Privacy-Aware Software Development
	• Security incident and event monitoring, security management
	  ○ Developing models for prediction/anticipation
	  ○ Improving risk-assessment (where to invest in security, run-time automatic security which balances need/risk/cost, fast understandable risk assessment, etc.)
	  ○ Improved Assurance Methods
	  ○ Development of tools for tracking data
	• Security systems
	  ○ Building systems that are resilient (vandal tolerance, bugs in software, resilience and failure tolerance, intrusion tolerant
	  ○ Handling systems issues (building secure cyber-physical systems providing/taking a holistic approach, making and maintaining models of complete systems, keeping mitigation up to speed with growth)
	  ○ Better language and tools for specifying secure software
	  ○ Standardisation of security features
	  ○ Development of rich and expressive security models
	• Mobile and emerging technologies
	  ○ Coping with deluge of devices: defences for mobile devices, securing sensor devices
	• Legal
	  ○ Enhancement of legislation to accommodate technological developments
	• Social
	  ○ Education of citizens, raising awareness in users of security and privacy risks

Internet Infrastructure Security and Resilience Reference Group


ROUTING THREATS
Autonomous System (AS) hijacking
Address space hijacking (IP prefixes)
Route leaks
BGP session hijacking
TIER 1 NETWORK
TIER 2 ISPs
IXPs
TIER 2 ISPs
TIER 3 ISPs
TIER 3 ISPs
TIER 3 ISPs
Internet users (business, consumers)
Nefarious Activity/ Abuse
Eavesdropping/ Interception/Hijacking


DNS THREATS
DNS registrar hijacking
DNS spoofing
DNS poisoning
Domain name collision
DNS Infrastructure
Nefarious Activity/Abuse


DENIAL OF SERVICE
DoS amplification/ reflection
DoS flooding
DoS protocol exploitation
DoS malformed packet attack
DoS application attack
INTERNET
Nefarious Activity/Abuse


NIS 4 Finance
Supply chain
Cloud Security Requirements
ISP / IXP Support
Secure Procure
Standard Technology
Backup Sources Provisionning
Preparedness
NIS FI-Guidelines
SDN security
Defense in Depth
SOC implementations
Secure ATMs
Secure Customers Devices
SecuRePay recommendations guidelines
Customer Facing Applications
Customer Education
Fraud Combat Prerequisites
Intelligence Sharing
Incident Detection
Logs Mining
Pattern Matching
Security configurations monitoring
SIEM
IDS
Threat Analysis Lab
Continuous Forensics
Victims support
Response
Retaliation
Cyberbullets avoidance
Collective Threat Response
EU Regulations impact
PSD2
NIS Directive
SecuRePay
National Regulations Convergence
Secure Customer Interactions
eIDAS
Real 2-factor
Using non-password auth
Biometrics
Smart cards
Mobile Phones
Phone call authentication
Transaction Security
Defense in Depth
Transaction Traceability
Standard data modeling (e.g. XML20022, FixML)
End-to-End integrity
Security Management Evaluation
Process Definition
Process Maturity
Certification
Risk transparence
Exercise
SOPs
Scenarii
x-border
x-sector
Training
Lessons Learnt

Department of homeland security/USA

Cyber threats: le infrastrutture critiche

(https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions)

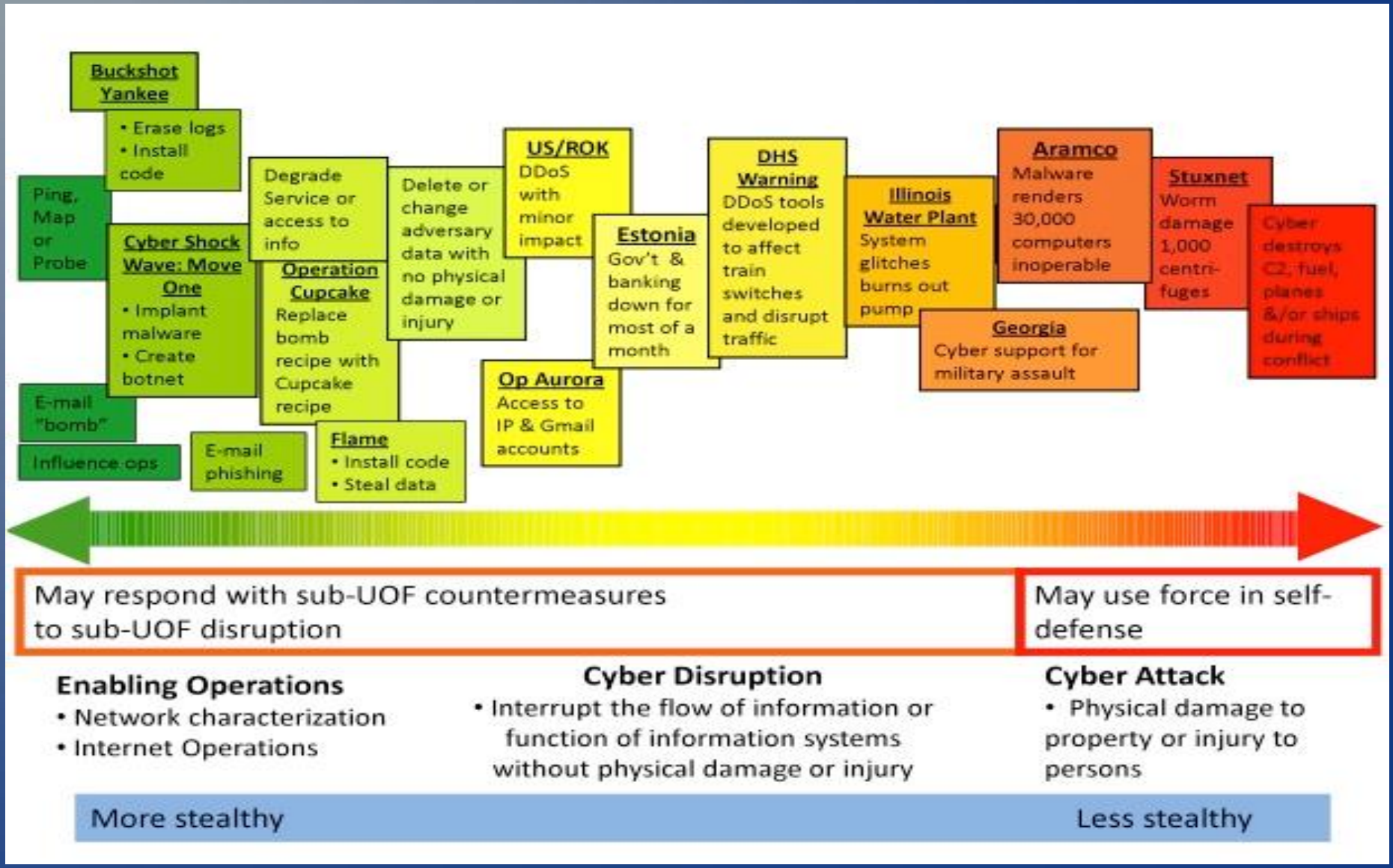
Cyber Descrizioni/fonti della minaccia

- **Le minacce informatiche a un sistema di controllo si riferiscono alle persone che tentano l'accesso non autorizzato a un dispositivo di sistema di controllo e / o di rete utilizzando un percorso di comunicazione dati.**
- **Questo accesso può essere diretto da all'interno di un'organizzazione da utenti fidati o da postazioni remote da parte di ignoti che usano Internet. Minacce per i sistemi di controllo possono provenire da numerose fonti, compresi i governi ostili, i gruppi terroristici, dipendenti scontenti e intrusi malintenzionati.**
- **Per proteggersi da queste minacce, è necessario creare una cyber-barriera sicura intorno al sistema di controllo industriale (ICS). Esistono altre minacce, comprese le catastrofi naturali, ambientali, un guasto meccanico e le azioni involontarie di un utente autorizzato.**

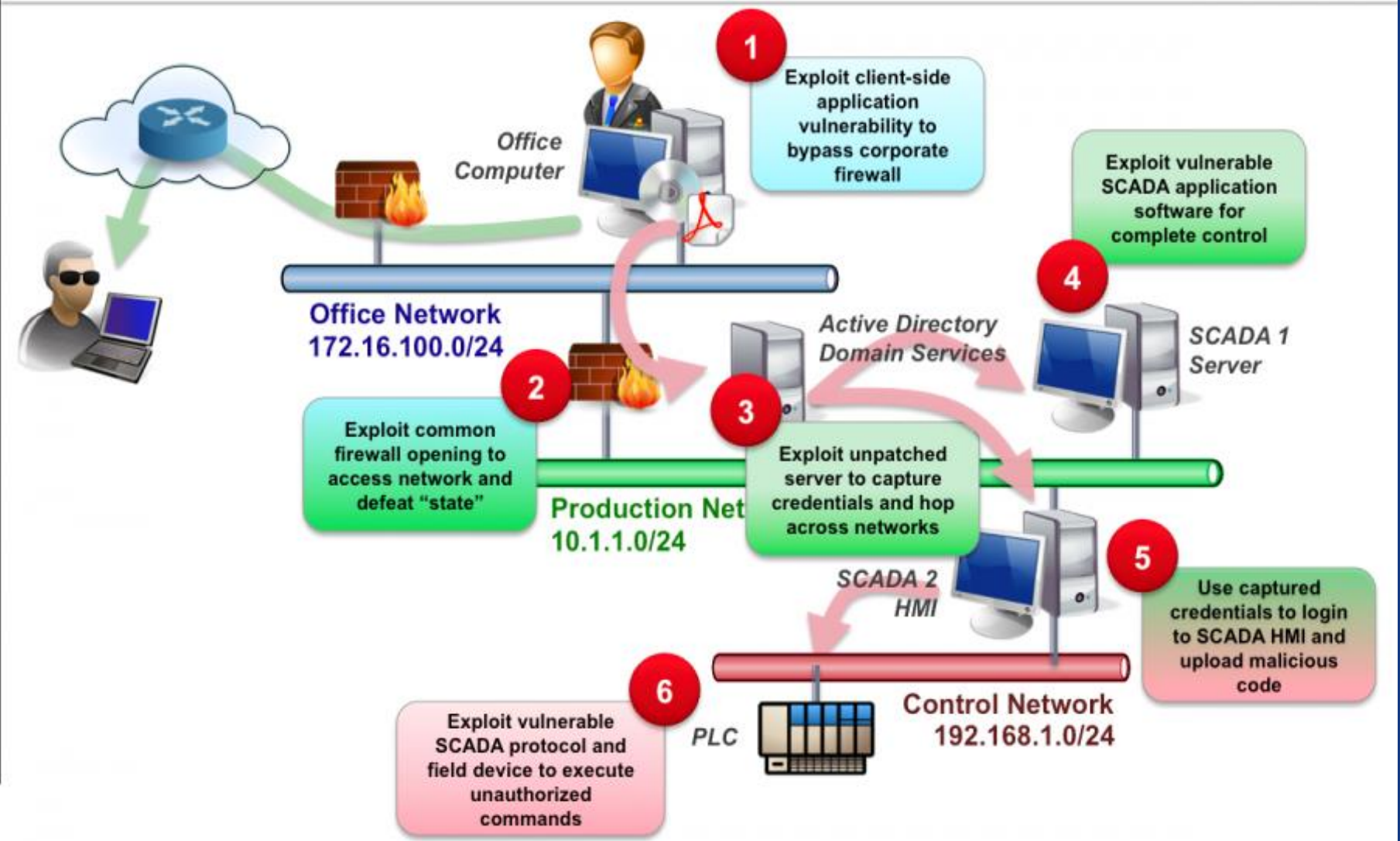
Tipi di infrastrutture critiche

Montage of pictures depicting various critical infrastructure sectors (from top left clockwise): drop of water hitting a body of water sending ripples out for the Water and Wastewater Sector; highway with cars beside traintracks with trains for the Transportation Systems Sector; antenna for the Communications Sector; server room for the Information and Technology Sector; storage tanks for the Chemical Sector; suspension bridge for the Transportation Systems Sector; and electric wires and electricty towers for the Energy Sector.

Attacchi alle infrastrutture critiche



Attack Demonstration



The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)/DHS (USA)

- responding to and analyzing control systems-related incidents;
- conducting vulnerability, malware, and digital media analysis;
- providing onsite incident response services;
- providing situational awareness in the form of actionable intelligence;
- coordinating the responsible disclosure of vulnerabilities and associated mitigations; and
- sharing and coordinating vulnerability information and threat analysis through information products and alerts.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

- governi nazionali
- terroristi
- spie industriali e gruppi criminali organizzati
- hacktivisti
- hacker
- GAO Threat Table

I governi nazionali

Il tradecraft necessario per impiegare efficacemente la tecnologia e gli strumenti rimane un importante fattore limitante, soprattutto contro obiettivi più difficili come reti classificate o infrastrutture critiche. Per i prossimi 5/10 anni, solo gli stati nazionali sembrano avere disciplina, impegno e risorse per sviluppare appieno le capacità di attaccare le infrastrutture critiche.

Il loro obiettivo è quello di indebolire, perturbare o distruggere gli Stati Uniti. I loro sotto-obiettivi includono lo spionaggio a fini di attacco; lo spionaggio per le tecnologie avanzate; interruzioni delle infrastrutture per attaccare l'economia americana; attacco su larga scala delle infrastrutture quando sono attaccati dagli Stati Uniti per danneggiare la capacità degli Stati Uniti di proseguire i suoi attacchi.

Terroristi

- Avversari terroristici tradizionali degli Stati Uniti, nonostante la loro intenzione di danneggiare gli interessi americani, **sono meno sviluppati nelle loro capacità tecnologiche e nella propensione a perseguire il cyber che non altri tipi di avversari**. E 'probabile, quindi, che pongano una minaccia cibernetica limitata.

- Dal momento che le bombe ancora funzionano meglio dei byte, i terroristi rimarranno probabilmente concentrati su metodi di attacco tradizionali nel breve termine. **Prevediamo altre minacce informatiche sostanziali siano possibili in futuro** come il fatto che una generazione più competente tecnicamente entri nei ranghi.

- Il loro obiettivo è quello di **diffondere il terrore in tutta la popolazione civile degli Stati Uniti**. I loro sotto-obiettivi includono: attacchi capaci di provocare 50.000 o più vittime all'interno degli Stati Uniti e attacchi per indebolire l'economia degli Stati Uniti e mettere in discussione la guerra globale al terrorismo.

Industrial Spies and Organized Crime Groups

- Spie aziendali internazionali e organizzazioni della criminalità organizzata rappresentano una minaccia di livello medio negli Stati Uniti attraverso la loro capacità di condurre spionaggio industriale e furto monetario su larga scala come pure la capacità di assumere o sviluppare degli hacker di talento.

- I loro obiettivi sono basati sul profitto. I loro sotto-obiettivi includono attacchi alle infrastrutture per il profitto di concorrenti o di altri gruppi di cui sopra, furto di segreti commerciali, accesso e ricatto dell'industria colpita con potenziale esposizione pubblica come minaccia.

Hacktivisti

Gli hacktivisti formano una piccola popolazione straniera di hacker politicamente attivi che comprende individui e gruppi con motivazioni anti-Usa . Essi rappresentano la minaccia di livello medio di effettuare un attacco isolato, ma dannoso. La maggior parte dei gruppi di hacktivisti internazionali appaiono orientati alla propaganda piuttosto che ai danni alle infrastrutture critiche. Il loro obiettivo è quello di sostenere la loro agenda politica. I loro sotto-obiettivi sono la propaganda e i danni che creano per ottenere notorietà per la loro causa

Hacker

Anche se le più numerose e pubblicizzate intrusioni informatiche e altri incidenti sono attribuiti a hacking-hobbisti solitari, questi hacker rappresentano una minaccia trascurabile di danni diffusi, a lungo termine a infrastrutture a livello nazionale.

- La grande maggioranza degli hacker non hanno la operatività per minacciare obiettivi difficili come reti critiche degli Stati Uniti e ancora meno avrebbero un motivo per farlo.

- Tuttavia, la grande popolazione mondiale di hacker pone un rischio relativamente alto di interruzione isolata o breve, che provochi danni gravi, tra cui gravi danni alle cose o la perdita della vita. Mentre la popolazione di hacker cresce, così cresce la probabilità di un hacker eccezionalmente esperto e malefico capace di riuscire in un simile attacco.

- Inoltre, il volume enorme in tutto il mondo di attività di hacking relativamente meno qualificato aumenta le possibilità di interruzione involontaria di un'infrastruttura critica.

La GAO Threat Table

The following table is an excerpt from NIST 800-82, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security (SME draft), provides a description of various threats to CS networks

GAO schema

Threat	Description
Bot-network operators	Bot-network operators are hackers; however, instead of breaking into systems for the challenge or bragging rights, they take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, or phishing attacks, etc.).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power - impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.

GAO cont

Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, who execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations who distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Spyware/malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005).

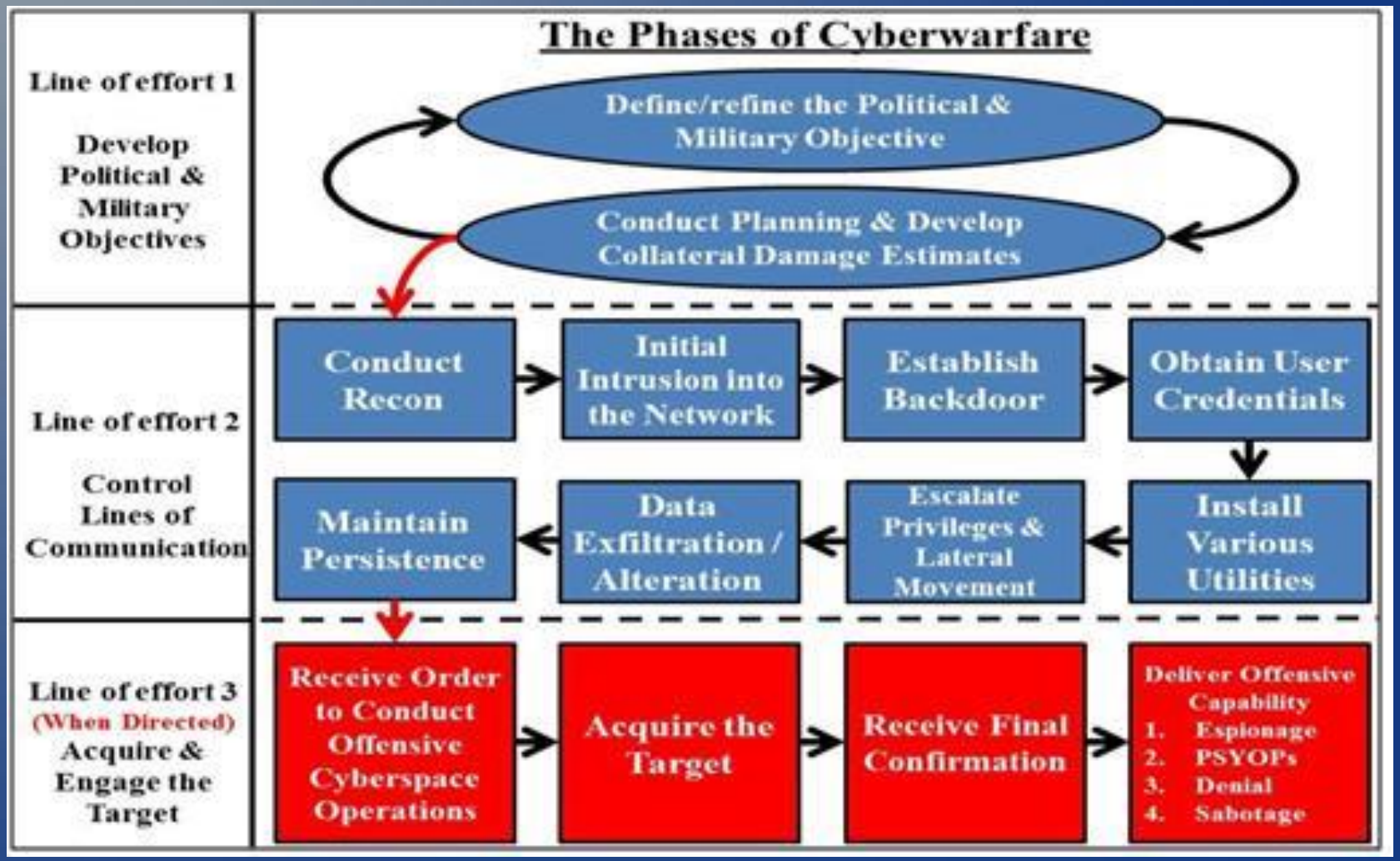
Cyber security threat prevention

Security boards

National strategies

- Ambito civile
- Ambito militare
- Ambito governativo
- Ambito industriale

La cyberwarfare



Military strategy

- parcellizzazione obiettivi
- microarticolazine delle competenze
- istituzione di nuovi organismi e funzioni
- scarso coordinamento interno
- sovrapposizione delle competenze
- mancanza di una cyber security diplomacy

La percezione e la previsione delle minacce

http://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2016

Survey Demographics

- 814 qualified IT security decision makers and practitioners
- All from organizations with more than 500 employees
- Representing 7 countries in North America and Europe
- Representing 19 industries

perceptions

The adequacy of existing cybersecurity investments, overall and within specific domains of IT

The likelihood of being compromised by a successful cyberattack within the next 12 months

The types of cyberthreats that pose the greatest risk to a given organization

The organizational factors that represent the most significant barriers to establishing effective cyberthreat defenses

The impact that software-defined networking (SDN) may have on an organization's ability to defend against cyberthreats

percezioni

The adequacy of existing cybersecurity investments, overall and within specific domains of IT

The likelihood of being compromised by a successful cyberattack within the next 12 months

The types of cyberthreats that pose the greatest risk to a given organization

The organizational factors that represent the most significant barriers to establishing effective cyberthreat defenses

The impact that software-defined networking (SDN) may have on an organization's ability to defend against cyberthreats

percezioni

The adequacy of existing cybersecurity investments, overall and within specific domains of IT

The likelihood of being compromised by a successful cyberattack within the next 12 months

The types of cyberthreats that pose the greatest risk to a given organization

The organizational factors that represent the most significant barriers to establishing effective cyberthreat defenses

The impact that software-defined networking (SDN) may have on an organization's ability to defend against cyberthreats

quesiti

Where do we have gaps in our cyberthreat defenses relative to other organizations?

Have we fallen behind in our defensive strategy to the point where our organization is now the "low-hanging fruit" (i.e., likely to be targeted more often due to its relative defensive weaknesses)?

Are we on track with both our approach and progress in continuing to address traditional areas of concern – such as strengthening endpoint security and reducing our attack surface – as well as tackling newer ones, such as providing security for mobility and defending against advanced persistent threats (APTs)?

How are other IT security practitioners thinking differently about cyberthreats and their defenses, and should we adjust our perspective and plans to account for these differences?

Percezione e previsione

Which of the following network security technologies are currently in use or planned for acquisition (within 12 months) by your organization to guard all network assets against cyberthreats? (*n=810*)

	Currently in use	Planned for acquisition	No plans
Network-based anti-virus (AV)	76%	16%	8%
Intrusion detection / prevention system (IDS/IPS)	69%	22%	9%
Secure email gateway (SEG)	69%	18%	13%
Secure web gateway (SWG)	63%	22%	15%
Denial of service (DoS) / distributed denial of service (DDoS)	59%	22%	19%
Security information and event management (SIEM)	56%	26%	18%
Next-generation firewall (NGFW)	54%	32%	15%
Web application firewall (WAF)	54%	28%	17%
Advanced malware analysis / sandboxing	53%	27%	21%
Data loss/leak prevention (DLP)	51%	31%	18%
Network behavior analysis (NBA) / NetFlow analysis	47%	30%	22%
Security analytics / full-packet capture and analysis	45%	33%	22%
Threat intelligence service	43%	32%	25%

<-- Less Frequency ---------- More Frequency -->

Table 1: Network security technologies in use and planned for acquisition

Research Highlights

Current Security Posture

- ☑ 70% of respondents are spending greater than 5% of their IT budgets on security. *(Pages 6-7)*
- ☑ 71% were affected by a successful cyberattack in 2014, but only 52% expect to fall victim again in 2015. *(Pages 7-9)*
- ☑ For the second consecutive year, mobile devices (smartphones and tablets) are perceived as IT security's weakest link, closely followed by social media applications. *(Pages 9-10)*
- ☑ Security analytics is the top-ranked network security technology planned for acquisition in 2015, followed by threat intelligence and next-generation firewalls. *(Pages 11-12)*
- ☑ Nearly a third lack tools to inspect SSL-encrypted traffic for cyberthreats. *(Pages 12-13)*
- ☑ Containerization/micro-virtualization technology is the top-ranked endpoint security and second-ranked mobile security technology planned for acquisition in 2015. *(Pages 13-15)*
- ☑ Only 23% of respondents are confident their organizations have made adequate investments to monitor the activities of privileged users. *(Pages 15-16)*

Perceptions and Concerns

- ☑ Phishing, malware, and zero-days give IT security the most headaches. *(Pages 17-18)*
- ☑ 59% of respondents experienced an increase in mobile threats over the past year. *(Pages 18-19)*
- ☑ Inadvertent exposure of confidential data is the top concern with SaaS-based file sharing applications. *(Pages 19-20)*
- ☑ Low security awareness among employees continues to be the greatest inhibitor to defending against cyberthreats, followed closely by lack of security budget. *(Page 22)*
- ☑ Nearly two-thirds of security professionals view SDN as having a positive impact on their ability to defend against cyberthreats. *(Page 23)*

Attack Surface Reduction

- ☑ Network access control (NAC) remains the top technology for reducing a network's attack surface. *(Pages 24-25)*
- ☑ Less than 40% of organizations conduct full-network active vulnerability scans more than once per quarter. *(Pages 25-26)*
- ☑ Only 20% of IT security professionals are confident their organizations have made adequate investments in educating users on how to avoid phishing attacks. *(Pages 27-28)*

Future Plans

- ☑ 62% of IT security budgets are expected to rise in 2015. *(Pages 30-31)*
- ☑ Although BYOD initiatives stalled in 2014, they are expected to nearly double in the coming year—from 30% to 59% of organizations. *(Pages 31-33)*
- ☑ More than two-thirds are looking to replace or augment current endpoint protection tools. *(Pages 33-34)*

Le previsioni di (in)sicurezza cyber

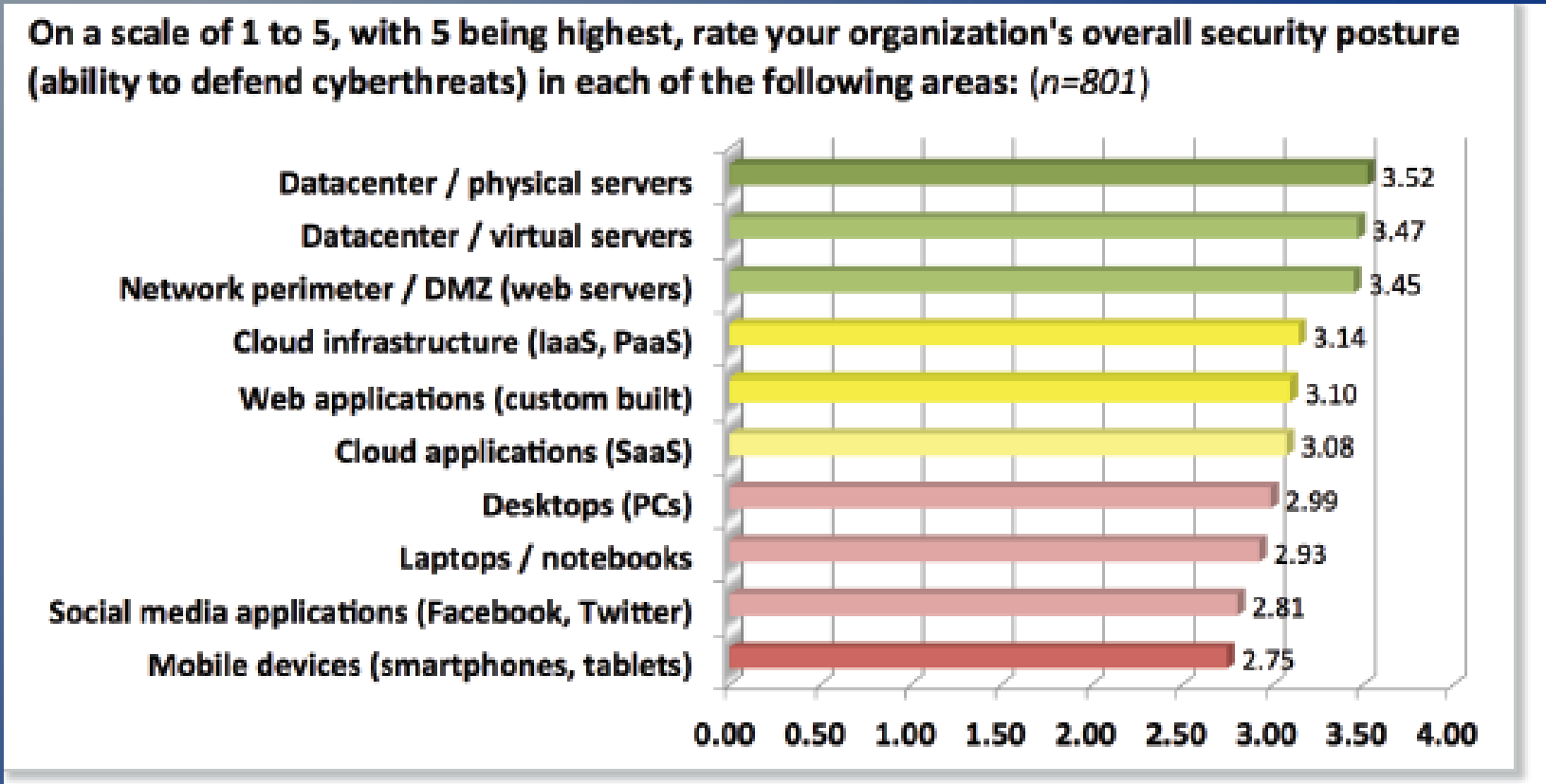


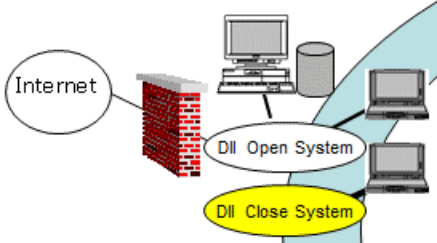
Figure 4: Perceived security posture by IT domain

② Development of protection system

(Network monitoring system, cyber defense analysis equipment, etc.)

① Enhancement of information communication system security

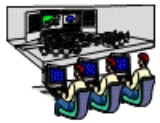
(Firewall and virus software, etc.)



③ Development of rules

(Execute "Instruction concerning the Protection of Ministry of Defense Information" and strengthen rules system, etc.)

Activities to promote education, Self Inspection, auditing, etc.



The 6 pillars of comprehensive cyber attack countermeasures

⑥ Research on the latest technologies

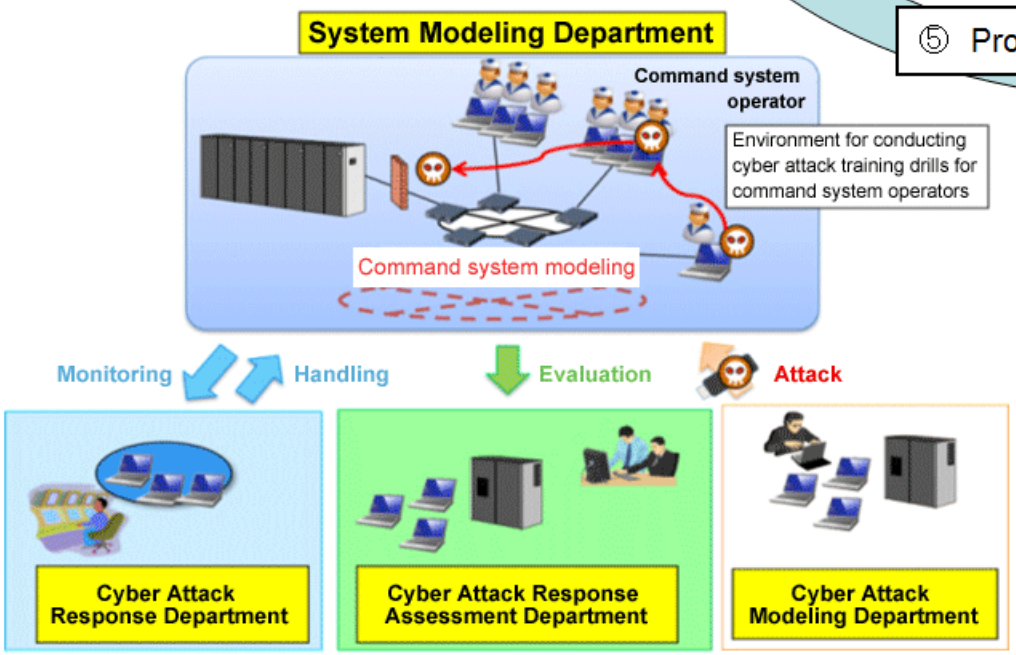
(Research into technologies for creating cyber attack practice environments, etc.)

④ Human resource development

(Study abroad at Carnegie Mellon University institutes and domestic graduate schools in Japan, provide specialized education at National Defense Academy of Japan, etc.)

⑤ Promotion of information sharing

(Collaboration with related ministries and agencies National Information Security Center and related countries such as the U.S., etc.)



L'agenda: i nodi e le soluzioni

Logiche internazionali

- Regole e visioni condivise: Nato, UE (la cybersecurity diplomacy)
- Coordinamento tra strutture nazionali e internazionali: *common policy* (europol, enisa, DHS, NIS, NSA, ecc.)
- Intelligence e dati (LEA e non solo)

Logiche di sistema

- La *security awareness* tipologica (persone, business, istituzioni, governo): il programma europeo Pe P(collaborazione pubblico e privato)
- La condivisione dell'informazione
- La competizione tecnologica
- L'integrazione tecnologica
- La ricerca
- Le strutture

L'efficacia delle azioni

- training operativo degli addetti: piani di formazione non spot, continuati, per tipologia di competenze (LEA, CERT, ecc.) e obiettivi
- *task force* interdisciplinari di livello, cllaborazioni pubblico-privato: ROSI, norme, comportamenti, *risk analysis*, *risk assessment*, soluzioni
- approcci preventivi e predittivi: nuovi modelli
- coordinamento degli organismi nazionali e internazionali

Piattaforme di servizi alla *cybersecurity*

- Progettazione e sviluppo dei servizi alla *cyber security*: allarmi, simulazioni, interventi risolutivi
- Analisi e monitoraggio attacchi
- Soluzioni *cyber security* specifiche
- Condivisioni dati
- Elearning applicativo
- Ontologia della *cybersecurity* e del *cyberthreat*
- Investimenti programmati e scalabili
- Iniziative joint pubblico-privato

Commenti e quesiti