infosecurity EUROPE

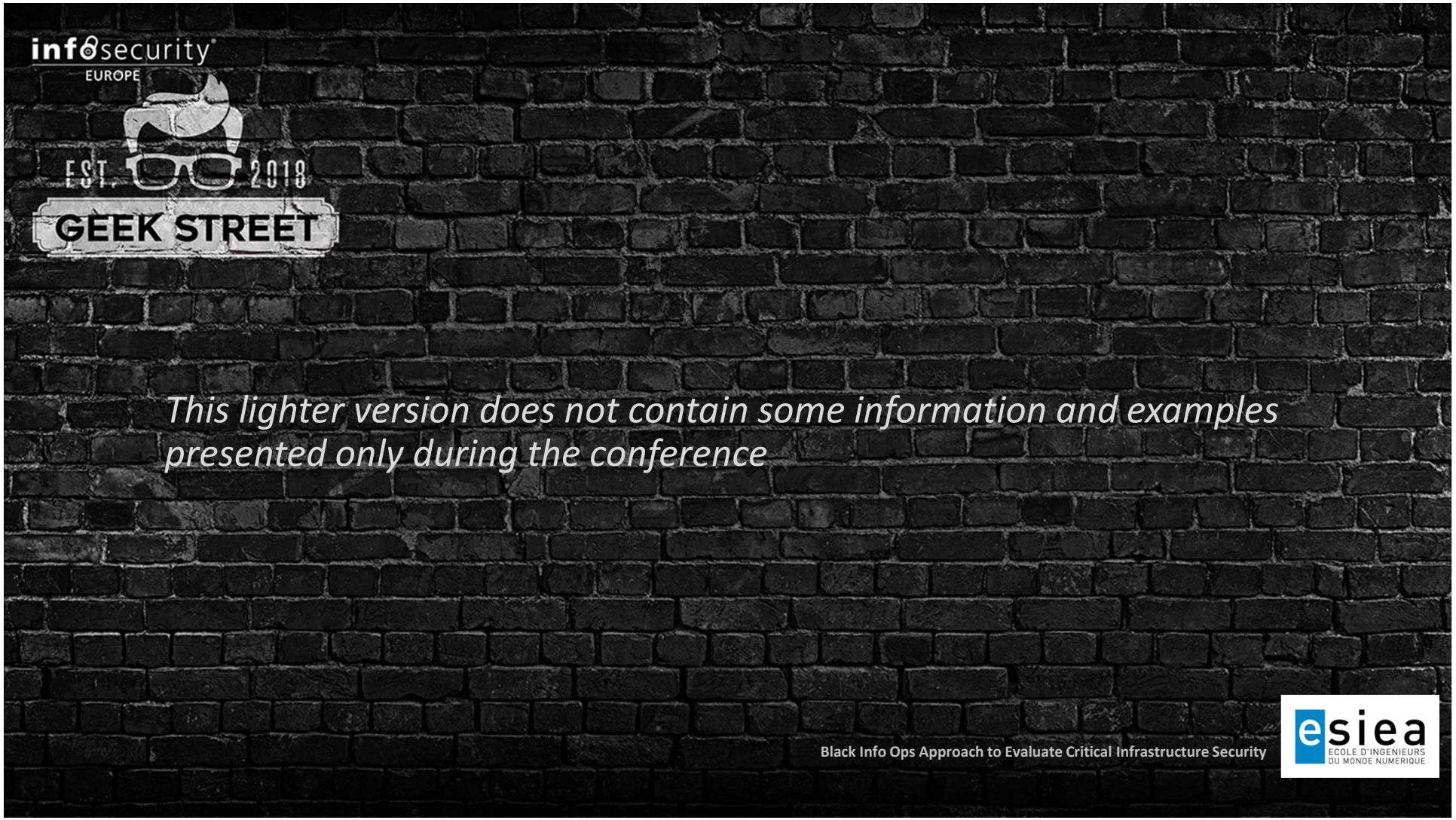
EST. 2018

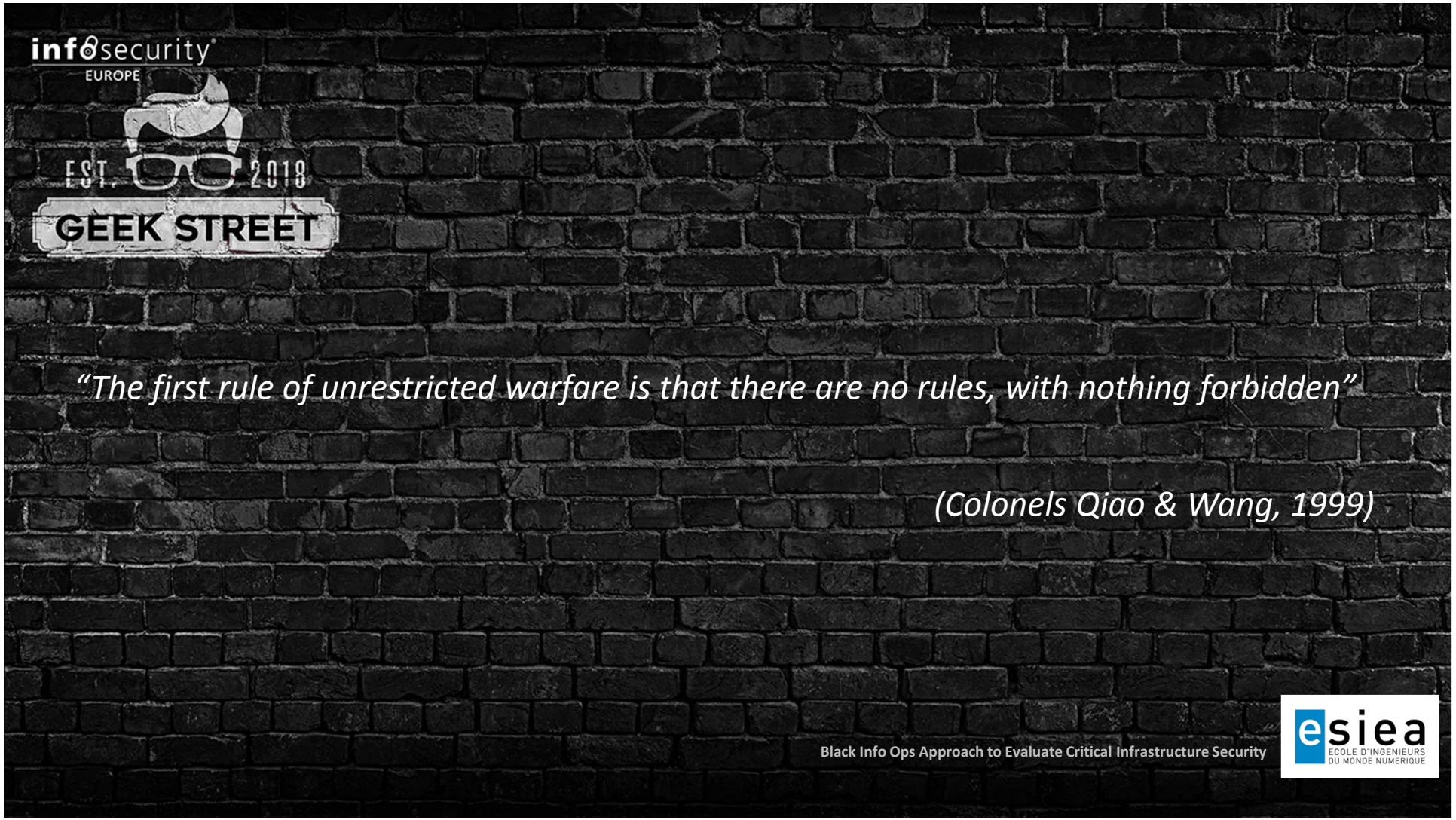
GEEK STREET

Prof. Eric FILIOL, Head of Research, ESIEA
filiol@esiea.fr – https://sites.google.com/site/ericfiliol

Black Info Ops Approach to Evaluate Critical Infrastructure Security

esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
This lighter version does not contain some information and examples presented only during the conference
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
"The first rule of unrestricted warfare is that there are no rules, with nothing forbidden"
(Colonels Qiao & Wang, 1999)
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

infosecurity EUROPE

My Background

- Scientific background (Ing. - Ph D - HDR) in mathematics and computer science.
- 22 years in the Army (French Marines Corps/Infantry)
  - Regimental period on the field ⇒ leadership training (platoon, company) and *Method of tactical reasoning* (MTR)
  - Technical operational positions in and around the intelligence domain ⇒ intelligence techniques, (offensive) (cyber)security
- NATO certifications
  - Information Operations Course (InfoOps; 2008) & Information Warning and Intelligence Systems (2004)
- Head of a research lab at ESIEA (https://en.esiea.fr/)
  - Research in (cyber) security with the attacker and/or hacker's perspective
- International consultant (operational security field)
- R\&D and analysis of many real cases/targets

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018

GEEK STREET

Agenda

- Introduction
- Black InfoOps
- General Methodology & Tools
- Case Study I - Security Analysis of the US Electric Grid
- Case Study II – How to Make a Military Operation Fail
- Conclusion

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018

GEEK STREET

Introduction

What Are We Speaking About?

What is the Context?

esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

infosecurity EUROPE

Introduction – What Are We Speaking About

- Global hysteria about “cyber”
  - If you are not “cyber” you do not exist! World of the cyber-everything
  - What about target that are not connected to anything
- In fact this is a limited and biased view
  - A lot of attacks are not/cannot be taken into account
  - For the Nation States, offers an easy but illusory management of problems in a difficult budgetary context
    - Justifies sliding towards citizens' mass surveillance (democracy or “democratorship”?)
    - Illustrative present day issue: total failure in Islamic terrorism management, recent actions against Nuclear Plants in France (2017)
    - History: terrorist attacks in the 80s/90s vs present day terror attacks
- The danger would be to badly prepared and protected against other forms of attacks
- Companies and economic entities must also be seen as critical infrastructures

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

The (cyber)World is Not Enough

- Cyber is just ONLY one more dimension but not necessarily the most prevalent one
- Main interest of cyber: intelligence step optimization and speed up, partially remove time and space.
  - Gathering a lot of information becomes easy (but greater noise and lower quality): open data, social networks (e.g collaborative espionage)...
  - Huge capability of analysis, processing and intelligence source
- For the attacker, the cyber tools/step may be the most unsure aspect (e.g. exploiting a 0-day against a server)
  - No serious operational would base an operation mainly on the cyber part

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

The (cyber)World is Not Enough (cont.)

- The optimal view of the Russian and Chinese doctrines
  - Information and operational field is far greater than the pure cyber field
  - Select a target, choose an effect to achieve on it, take the most convenient tools/techniques to succeed
  - Present day paradigm of attacks: the impersonation of the leader to embezzle company's money.
- Adopt a larger view in time and space
- Fundamental error: to confuse goal and means/tools.
- True target: humans and assets not computers
- Fact: it is impossible to prove that any protection/defence is efficient. It is always to prove that an attack is possible: just do it

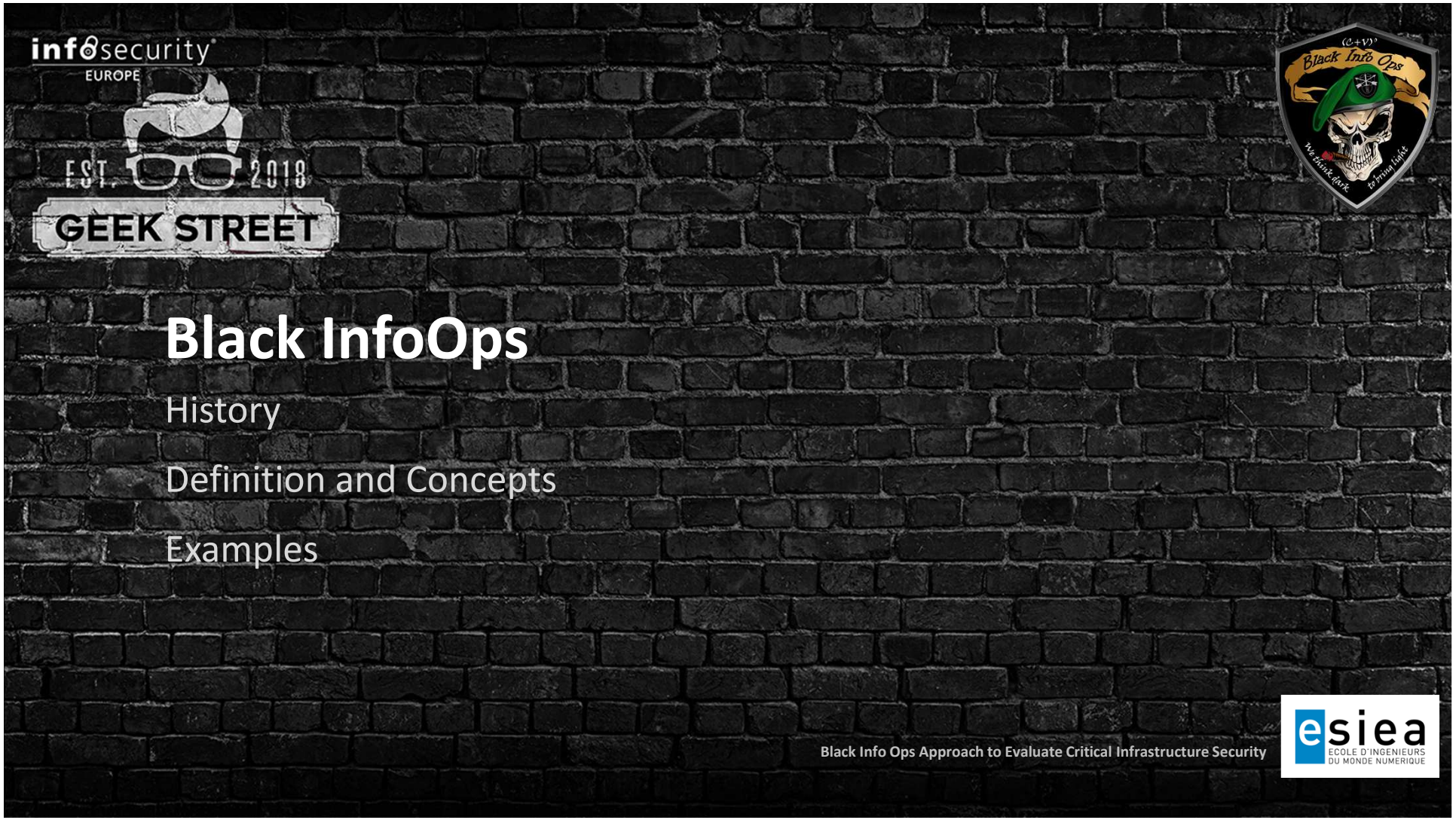
esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Aim of Research

- Evaluate the actual security of any systems and especially large critical infrastructures
  - For attackers, there is no such thing as Ethics or state of soul: as far as attacks are concerned there are those that succeed and those that fail
- Combine the perspective/greed of the attackers and the power of InfoOps
  - Black InfoOps: InfoOps + warfare art and techniques + hacking tools + intelligence tools
- Formalization approach to enable automated pre-processing and generalized attack paths identication.
  - See my research papers in the bibliography section

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Black InfoOps
History
Definition and Concepts
Examples
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

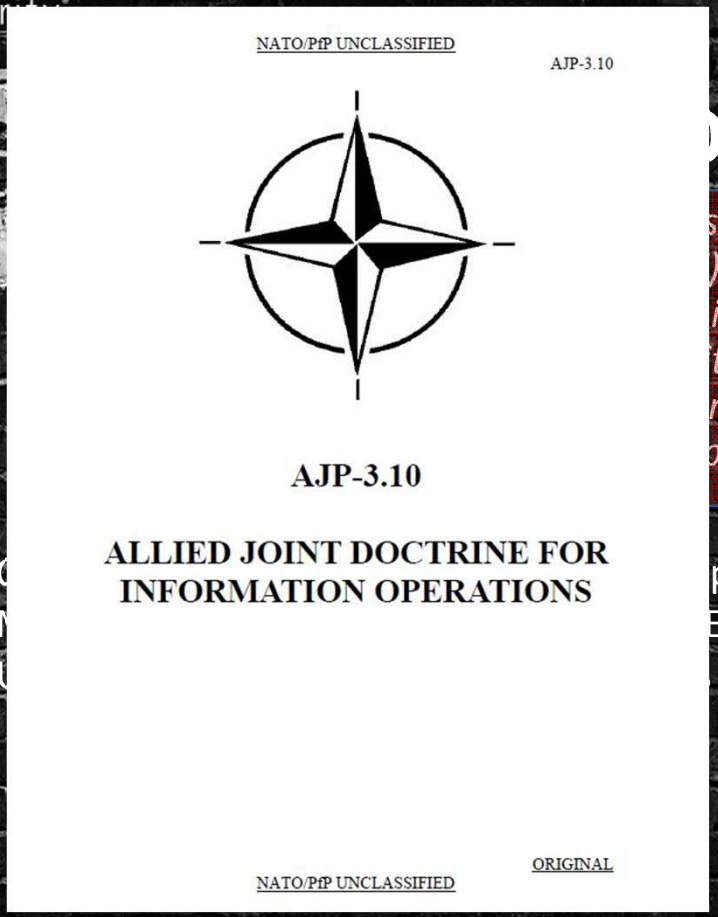
infosecurity EUROPE

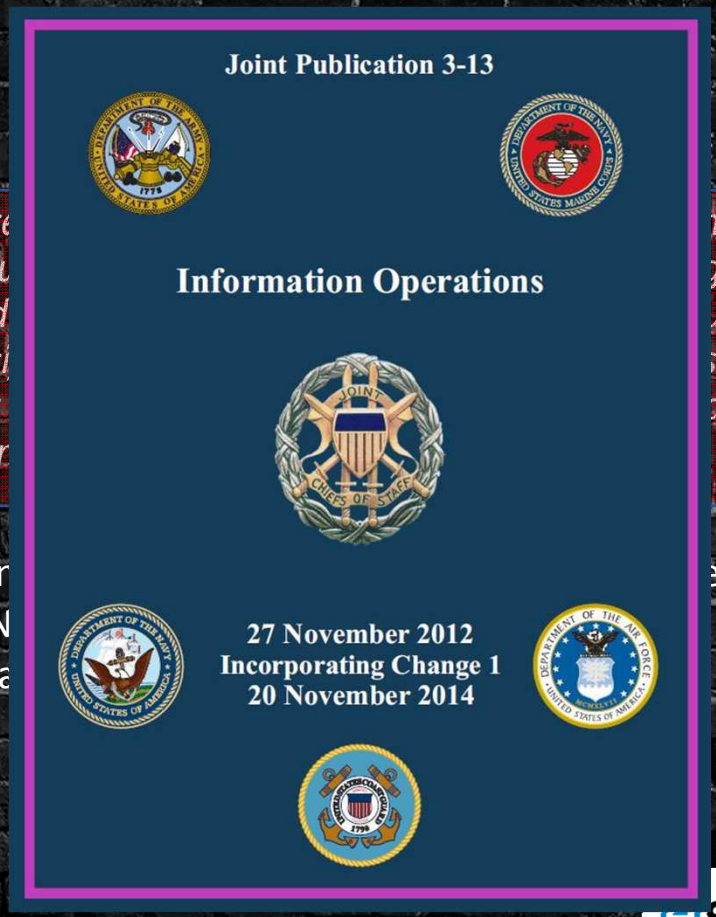
NATO InfoOps

Information Operations - IO are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

- Category of direct and indirect support operations for the United States Military. Published by NATO as AJP 3.10 ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS" (2009)
- US Army version as JP 3.13 (Joint Staff) as Information Operations" (2012, modified 2014).

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE


NATO/PfP UNCLASSIFIED
AJP-3.10
AJP-3.10
ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS
ORIGINAL
NATO/PfP UNCLASSIFIED


Joint Publication 3-13
Information Operations
27 November 2012
Incorporating Change 1
20 November 2014

infosecurity EUROPE

InfoOps Examples

- Lebanon conflict (2006)
- Case study (US):
  - https://publicintelligence.net/ufouo-u-s-marine-corps-information-operations-april-2010/
- Case study (Russia):
  - http://www.europeanvalues.net/kremlin-watch-briefing-west-learn-baltics/
- Still ongoing operations (US & Russia): Syrian conflict, Ukrainia crisis, Skripal case, Iranian crisis...

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

InfoOps - Pros & Cons

- Pros & Strengths
  - Global view
  - Joint coordination of different means/domains and actors
  - Use of the intelligence domain.
- Cons and Limitations
  - Still too restricted. Does not take the full domain possible (e.g. physical domain). Soft targets only
  - Limited effects (target: information and mind)
  - Limited efficiency wrt accountability concerns (the operation must be neither traced nor attributed). Ideally the operation itself must be invisible
  - Requires to be superior (politically, technologically...) to the target, opponents or even allies
  - Must be compliant with international and local regulations

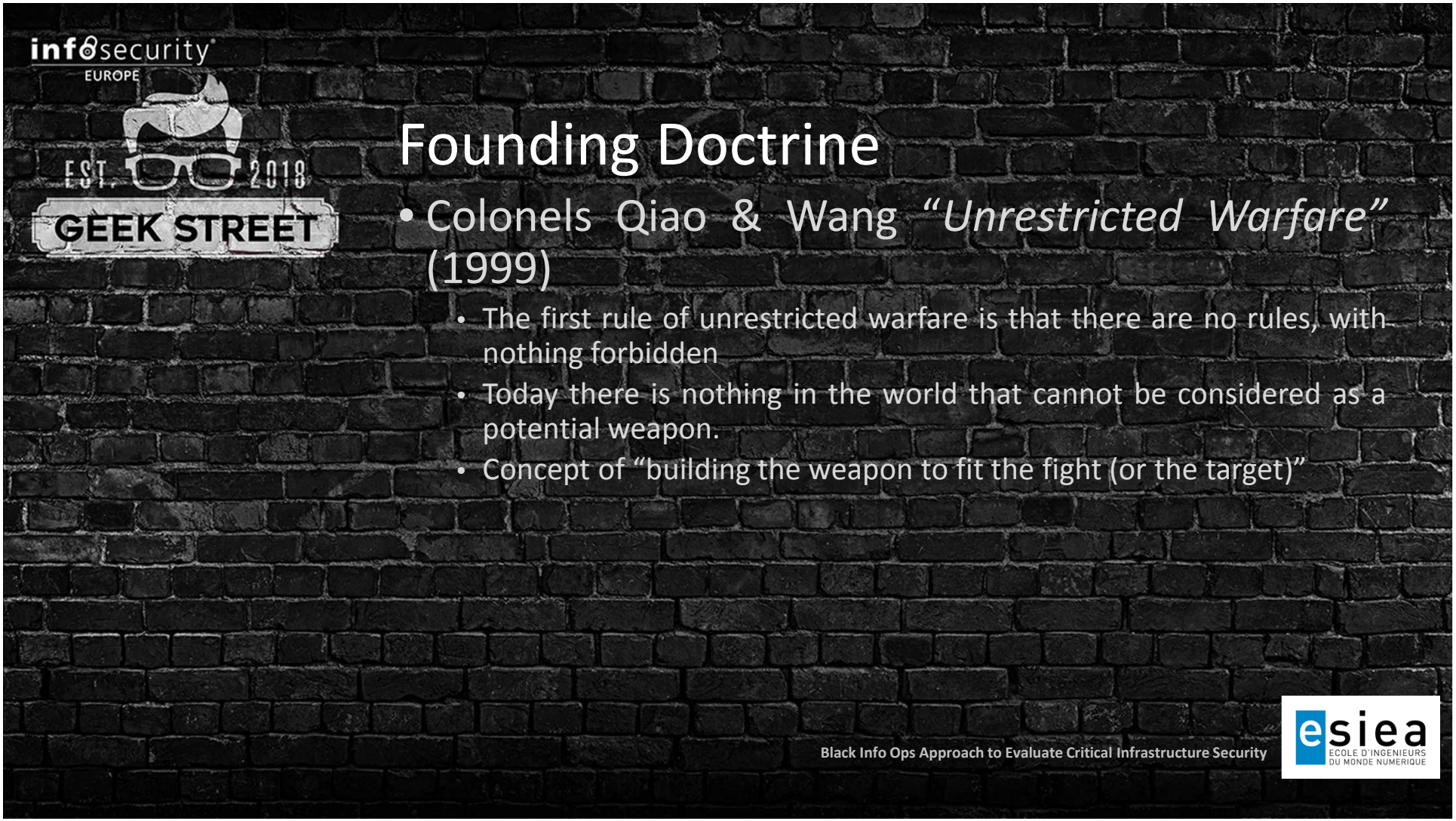
esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Black InfoOps

- Term coined to describe the set of total war and attack techniques
- Combines
  - Classical InfoOps approach
  - Russian and more recently Chinese doctrines
  - Terrorists' approach
  - Hackers' approach (only the result matters not the method)
  - Intelligence and military warfare techniques
  - Exploit all aspects (cultural, sociological, psychological, emotional...) of the target environment

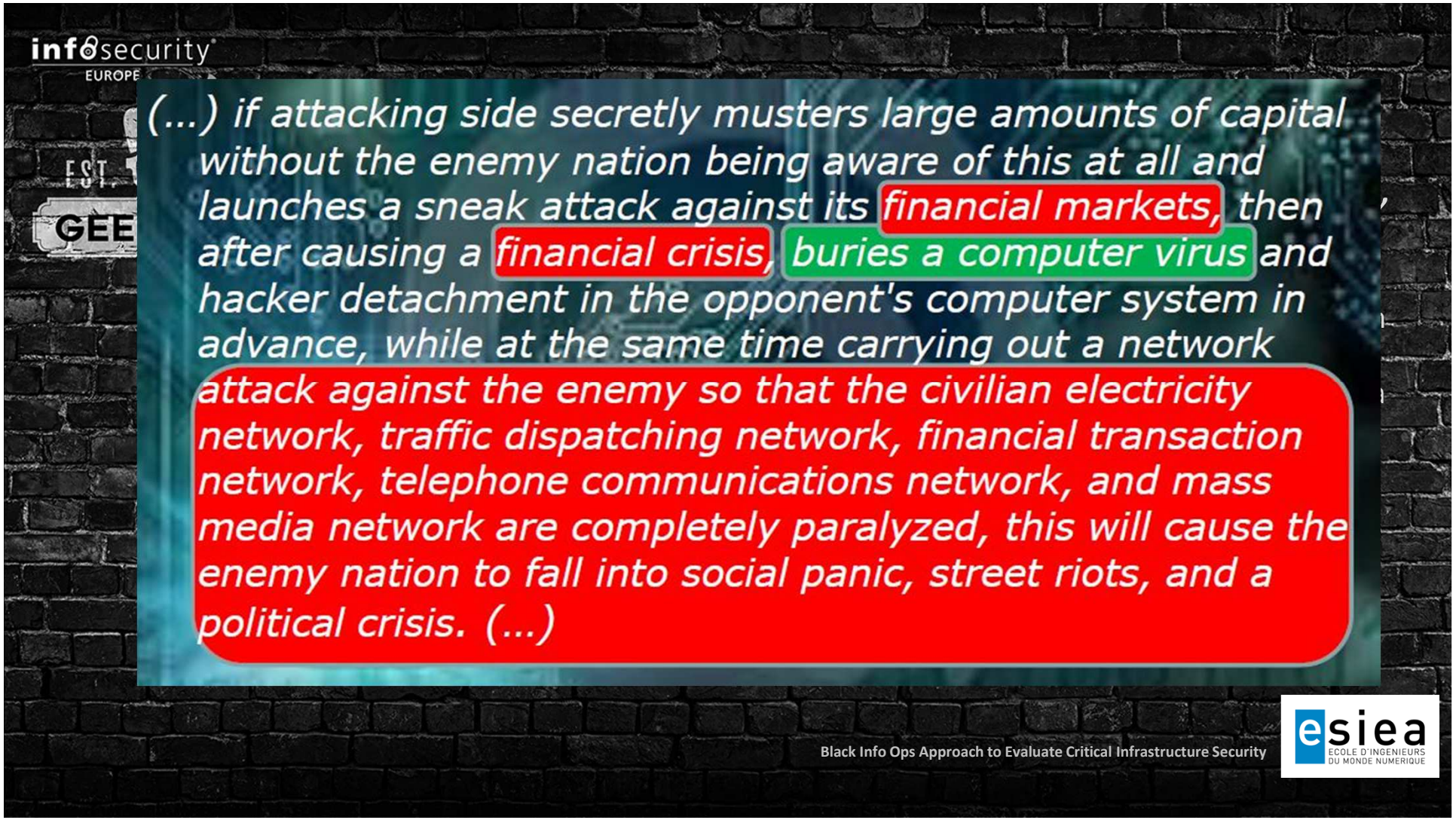
esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

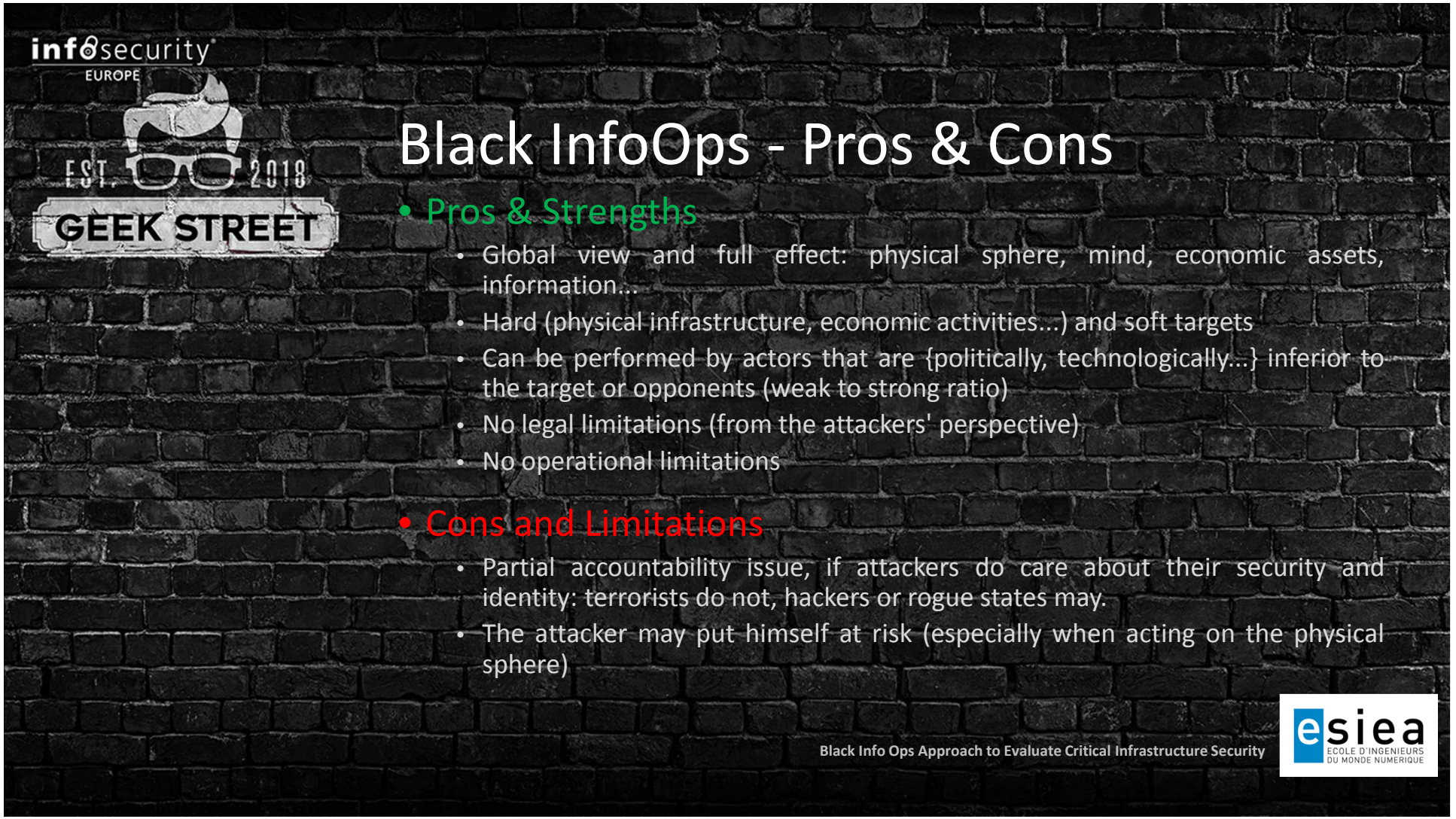


Founding Doctrine

- Colonels Qiao & Wang *"Unrestricted Warfare"* (1999)
  - The first rule of unrestricted warfare is that there are no rules, with nothing forbidden
  - Today there is nothing in the world that cannot be considered as a potential weapon.
  - Concept of "building the weapon to fit the fight (or the target)"

esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
(...) if attacking side secretly musters large amounts of capital without the enemy nation being aware of this at all and launches a sneak attack against its financial markets, then after causing a financial crisis, buries a computer virus and hacker detachment in the opponent's computer system in advance, while at the same time carrying out a network attack against the enemy so that the civilian electricity network, traffic dispatching network, financial transaction network, telephone communications network, and mass media network are completely paralyzed, this will cause the enemy nation to fall into social panic, street riots, and a political crisis. (...)
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Black InfoOps - Pros & Cons
• Pros & Strengths
• Global view and full effect: physical sphere, mind, economic assets, information…
• Hard (physical infrastructure, economic activities…) and soft targets
• Can be performed by actors that are {politically, technologically…} inferior to the target or opponents (weak to strong ratio)
• No legal limitations (from the attackers' perspective)
• No operational limitations
• Cons and Limitations
• Partial accountability issue, if attackers do care about their security and identity: terrorists do not, hackers or rogue states may.
• The attacker may put himself at risk (especially when acting on the physical sphere)
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

infosecurity EUROPE

Black InfoOps - Identified Cases

- Estonia (2007)
- Crimea (Nov. 2015)
  - https://www.nytimes.com/2015/11/23/world/europe/power-lines-to-crimea-are-blown-up-cutting-off-electricity.html
- A few other recent cases: USA 2012, China 2017, France 2017...(alas non public and/or under current investigation)
- Generally, the few known cases do not exploit all the power of Black InfoOps due to lack of methodology, of care and of tactical refinement.

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

Identified Cases

015/11/23/world/europe/power-lines-to-crimea-

2017…(alas non public

- Generally, the few kno
of Black InfoOps due t
tactical refinement.


infosecurity
EUROPE
EST. 2018
GEEK STREET
Black Info Ops
General Methodology
Operational Steps
Key Features
Target Graph & Connectivity
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

infosecurity EUROPE

Aims

- Choose a target (critical infrastructure) and an effect to create on it
- The attack must be perceived as sudden and immediate (prevent all warning signals)
- Minimize the attackers efforts. The actors and means used during the attack itself must be reduced as much as possible
- Maximize the time for the target to understand what happened and to recover. Optimally, it may be necessary to ensure that the attack is attributed to a third party
- Protect as much as possible the attackers (identification, exfiltration)

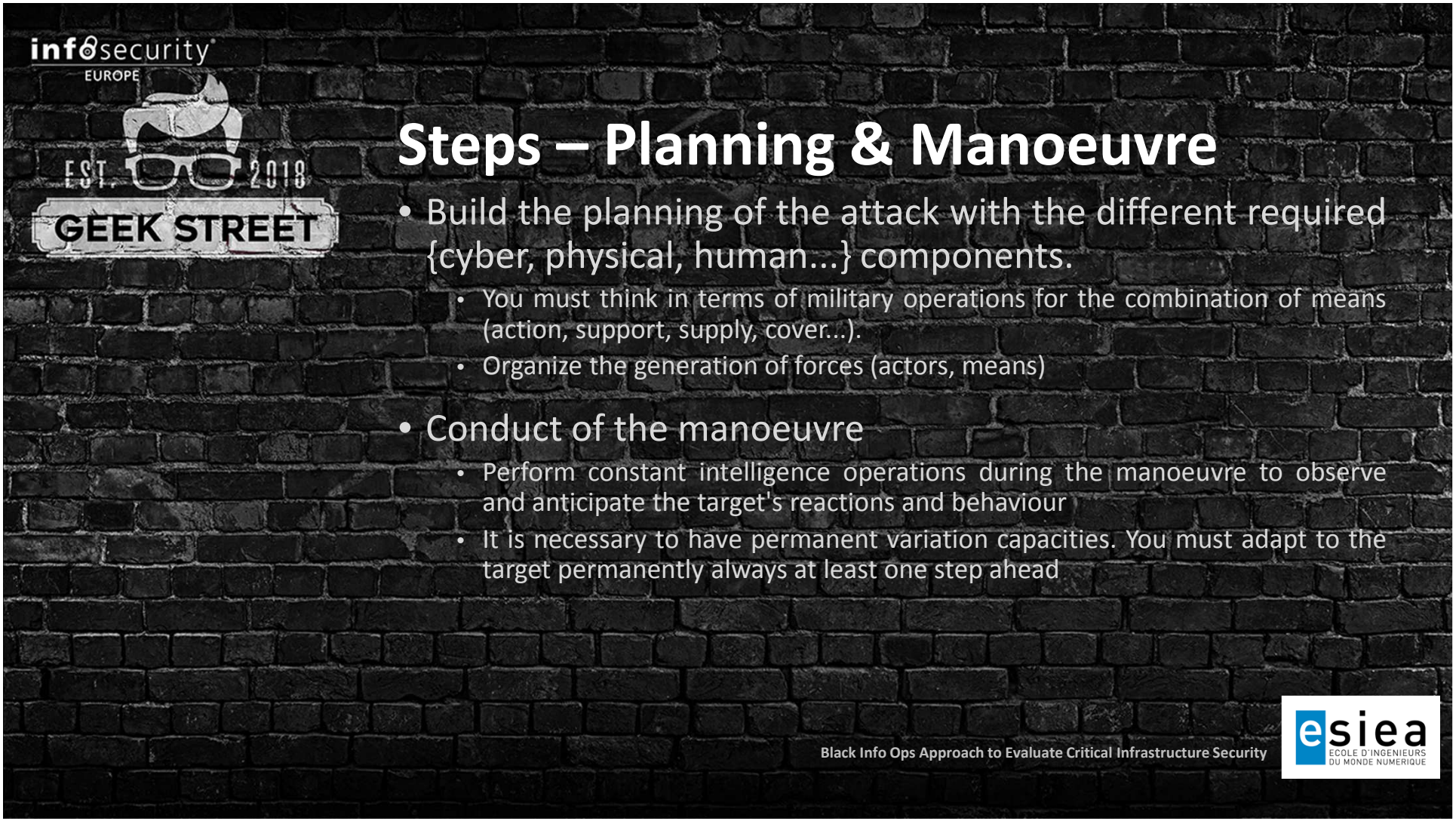
esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Steps – Intelligence

- Identification of all exploitable weaknesses (informational, physical, IT, human, organisational, environment...)
  - Maximal use of data collection (OSINT, HUMINT, SIGINT, ELINT...)
  - Exploit the huge potential of Open Data
  - Perform an extensive data analysis (intelligence step). Most of the sensitive data are derived from innocent-looking, non sensitive data.
  - Use the power of data science

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Steps – Planning & Manoeuvre
• Build the planning of the attack with the different required {cyber, physical, human...} components.
• You must think in terms of military operations for the combination of means (action, support, supply, cover...).
• Organize the generation of forces (actors, means)
• Conduct of the manoeuvre
• Perform constant intelligence operations during the manoeuvre to observe and anticipate the target's reactions and behaviour
• It is necessary to have permanent variation capacities. You must adapt to the target permanently always at least one step ahead
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018

GEEK STREET

Key Feature I - Domino Attack Principle

- The attack must be thought like an initial impulse creating a domino effect.
- This initial impulse must be naturally amplified by the self-amplifying ability of the target and its environment
- Minimizes the attacker's efforts and reduce its own exposure risk

Examples

- Perform zone control or social disruption using the crowd (Watts Riots, 1965; France 2005 - 2010; racial riots USA). See my Brucon 2009 talk - Strikes that block vital economic entities or resources

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018 GEEK STREET

Key Features II

- The larger the target or its environment the greater the domino effect and the self-amplifying properties are possible and important.
  - Increase the size of the attack graph and play on its connectivity (see further)
- The further away from the target, the less imputable the attack, but the stronger the domino effect must be
- As a corollary, third-party targets may be involved due to their functional critical link with the primary target (see Case Study II)
  - As a target, I have to determine whether I am a critical third-party component for others (must be included in my BCP)

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018 GEEK STREET

Key Features III

- Understand the environment specificities and features
  - The sociological and cultural characteristics must be understood precisely.
  - What is possible in a country may be not in another country.
- Examples
  - Instrumentation of trade/labor union staff: favorable to the attacker in countries like France, Spain, Italy... but not in countries such as Germany or the USA
  - Finding explosive and arms: easy in the USA, Russia, Central Europe but difficult to very difficult in Western or Northern Europe.
  - Misc.: age and state of infrastructures, availability of qualified staff, budgetary difficulties, climatic events...

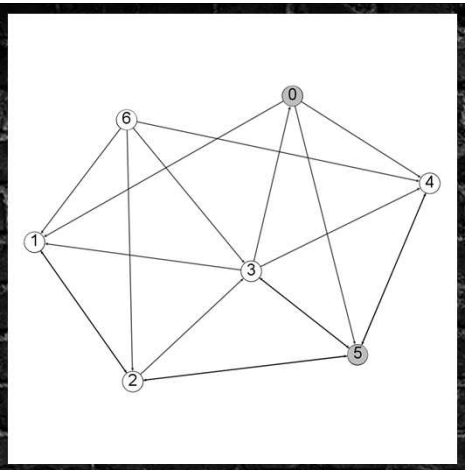
esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Key Features IV

- As much as possible, create and exploit an asymmetry in favour of the attacker that will disrupt the possibilities of reaction or protection of the target or law enforcement
  - Ex. 1: when facing a strike or riot, the state or target is limited in its possibility of reaction (societal or ideological asymmetry)
  - Ex. 2: in a democratic state, the management of journalists or activists is delicate (strong media impact, political asymmetry)
  - Ex. 3: the cost or conditions of recovery are tremendously hindering the defence side (economic asymmetry)

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE



Target Graph

- Target C_0 and its environment (external components C_1 to C_6) as a dependency graph.
- Each C_i can itself be decomposed into a similar graph. These components are physical, human parts, services...
- Dependence matrix A

C_0

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

Initial matrix

$$\begin{bmatrix} 37 & 104 & 88 & 87 & 99 & 93 & 39 \\ 20 & 58 & 57 & 51 & 61 & 51 & 19 \\ 51 & 147 & 128 & 127 & 141 & 132 & 57 \\ 51 & 144 & 127 & 124 & 141 & 127 & 53 \\ 20 & 57 & 46 & 47 & 52 & 53 & 23 \\ 47 & 136 & 133 & 122 & 143 & 119 & 46 \\ 56 & 161 & 152 & 142 & 165 & 141 & 56 \end{bmatrix}$$

93 dependencies of depth 5 between C_0 and C_5

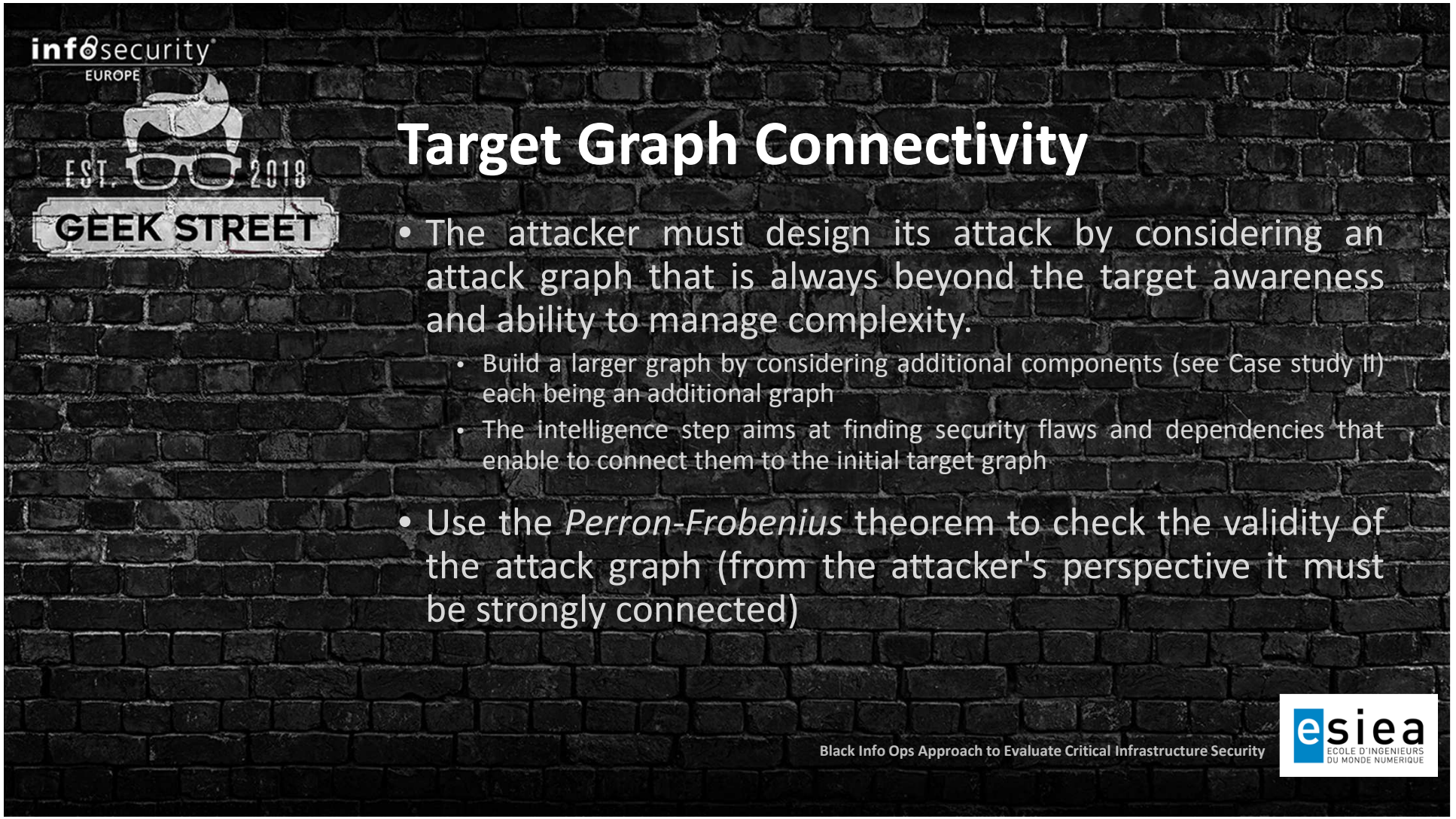
infosecurity EUROPE

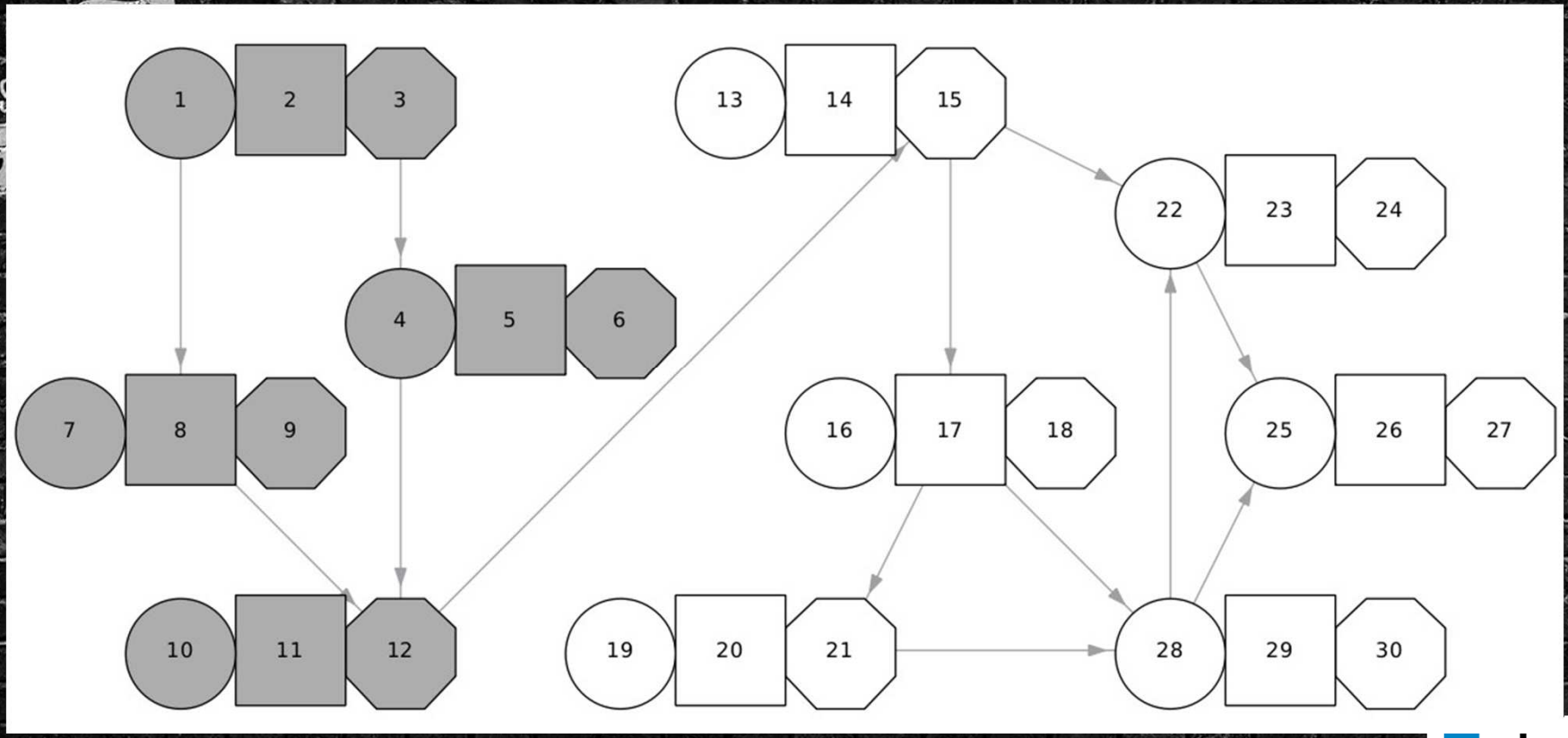
EST. 2018 GEEK STREET

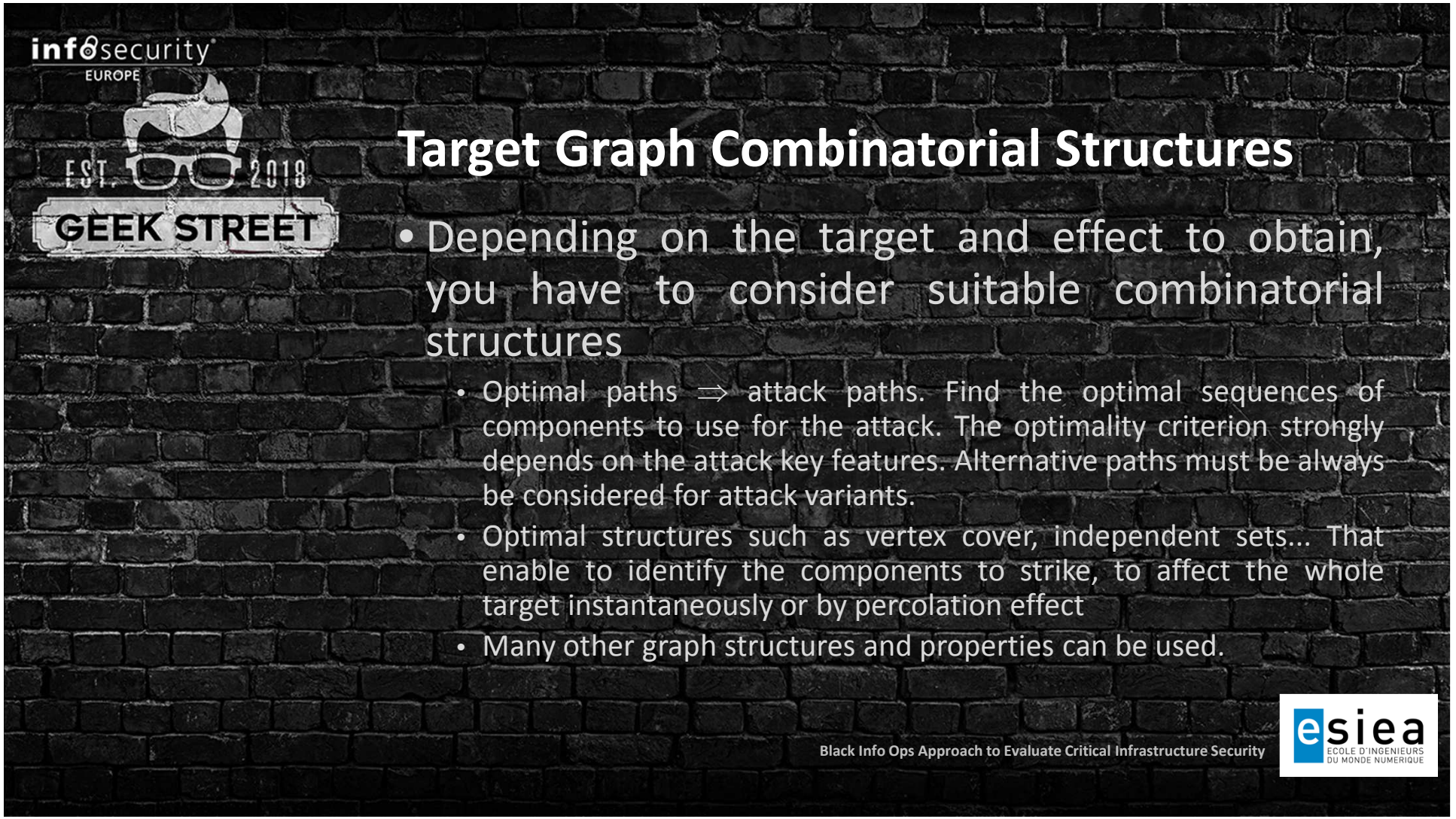
Target Graph (2)

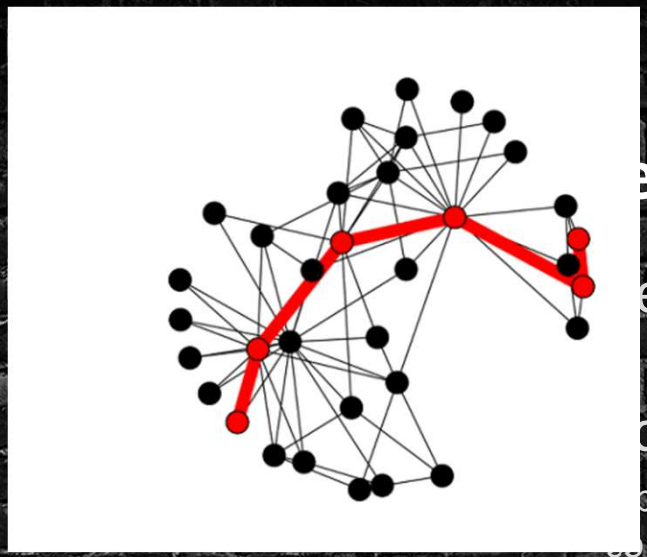
- In both cases, there exist a dependency chain between the target C_0 and component C_5
  - Component C_5 is not protected enough against attacks.
  - By attacking C_5, the attacker tries to obtain a “domino effect” by exploiting the existing (unforeseen) dependencies
- In real cases (dense dependencies), the number of possibilities is such
  - that there exist a large number of “variants” for the attacker (planning and conduct of manoeuvre phases)
  - The mapping is far too complex for the defender to analyse and to provide a strong and aware enough defence of target C_0.

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

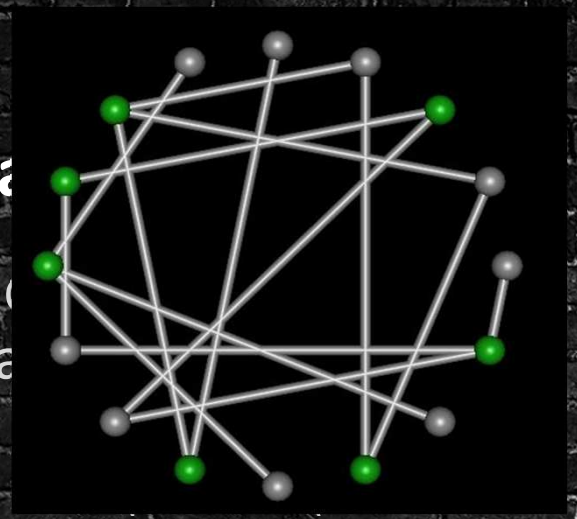

infosecurity
EUROPE
EST. 2018
GEEK STREET
Target Graph Connectivity
• The attacker must design its attack by considering an attack graph that is always beyond the target awareness and ability to manage complexity.
• Build a larger graph by considering additional components (see Case study II) each being an additional graph
• The intelligence step aims at finding security flaws and dependencies that enable to connect them to the initial target graph
• Use the *Perron-Frobenius* theorem to check the validity of the attack graph (from the attacker's perspective it must be strongly connected)
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE


1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

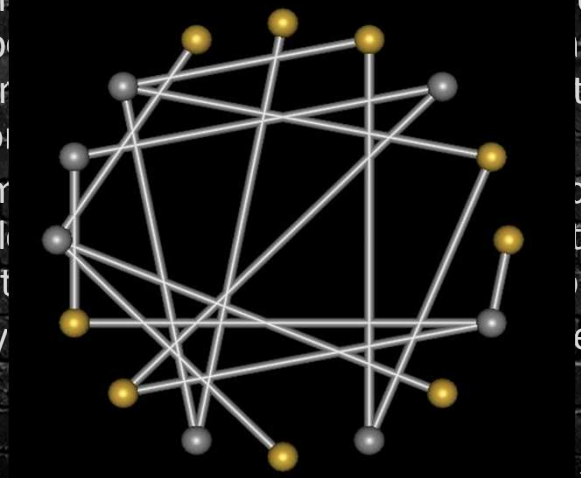

infosecurity
EUROPE
EST. 2018
GEEK STREET
Target Graph Combinatorial Structures
• Depending on the target and effect to obtain, you have to consider suitable combinatorial structures
• Optimal paths ⇒ attack paths. Find the optimal sequences of components to use for the attack. The optimality criterion strongly depends on the attack key features. Alternative paths must be always be considered for attack variants.
• Optimal structures such as vertex cover, independent sets... That enable to identify the components to strike, to affect the whole target instantaneously or by percolation effect
• Many other graph structures and properties can be used.
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE



et Graph Combinatoria



ending on the target an
have to consider suita
ctures



e optimality criterion strongly
ternative paths must be always

- Optim
  over, independent sets... That
  enabl
  to strike, to affect the whole
  target
  n effect
- Many
  erties can be used.

to Evaluate Critical Infrastructure Security

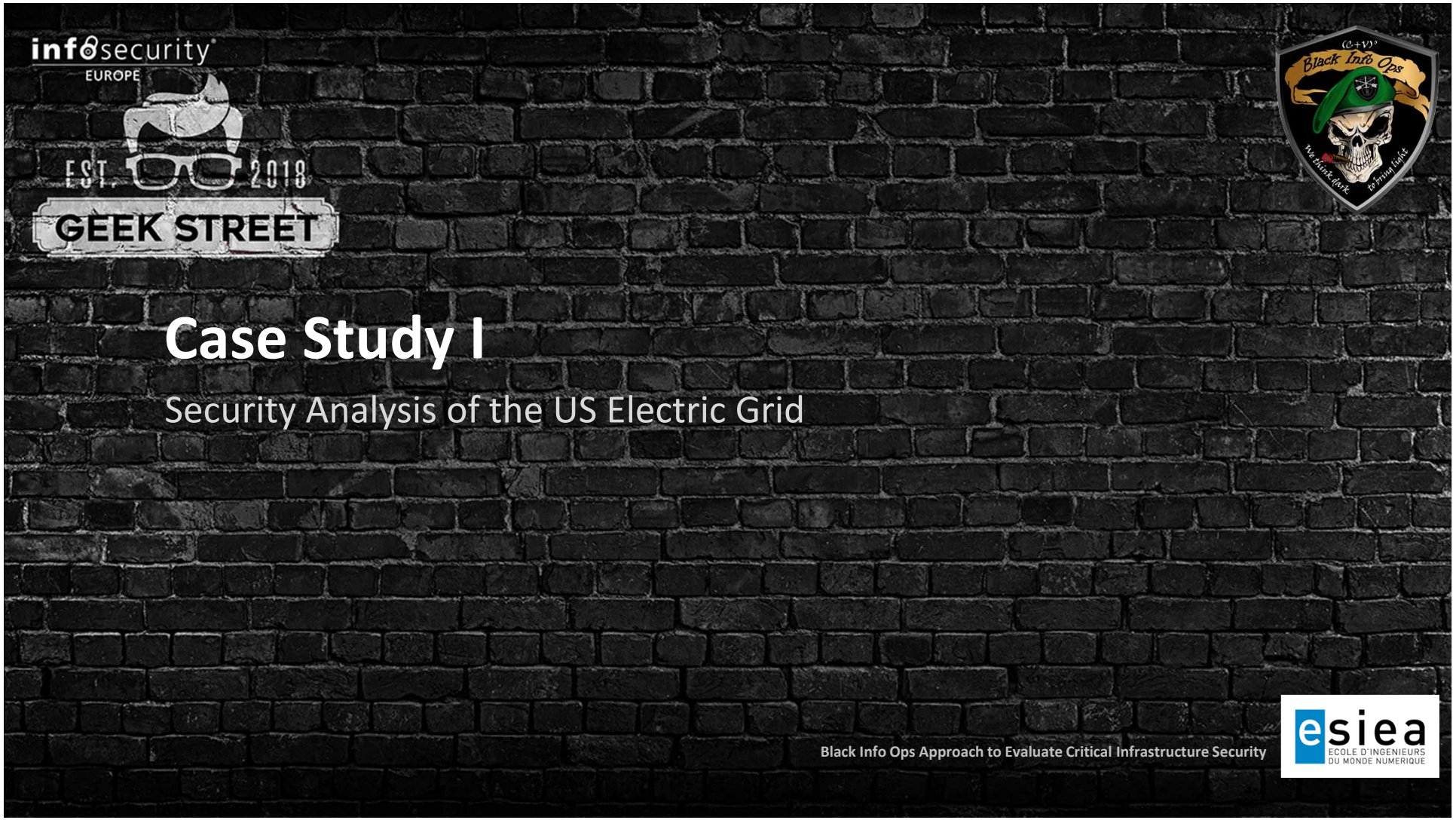
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

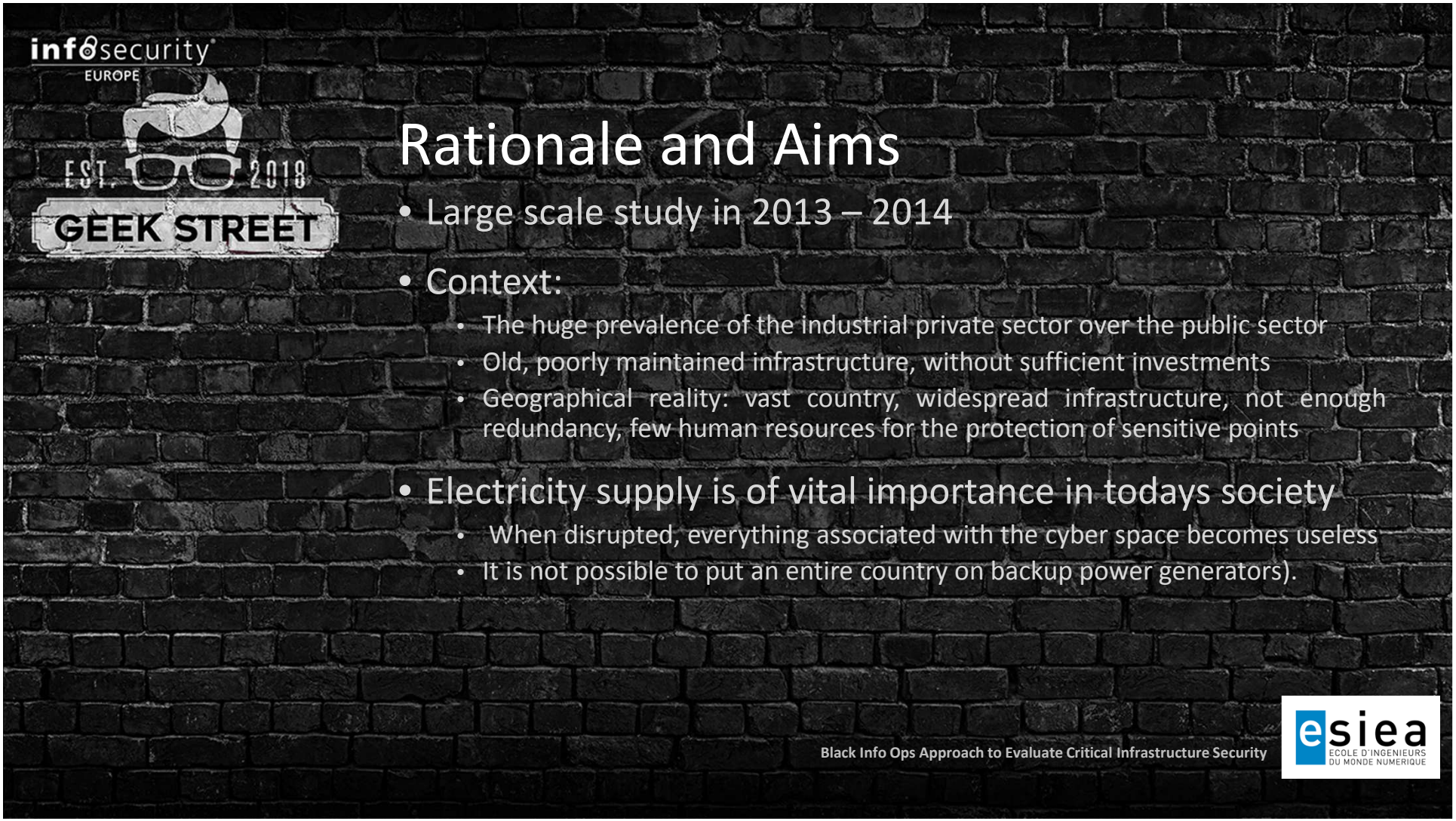
infosecurity EUROPE

Case Studies

- Let us now analyze two case studies, I have worked on.
  - US Electric Grid (initial physical target) ⇒ economic and social disruption (final effect after amplification)
  - Critical economic entities (initial target) ⇒ Military operation (final functional target)
- Any target (critical infrastructure, economic entities of any size, political entities…) should be analysed according to Black InfoOps approach

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Case Study I
Security Analysis of the US Electric Grid
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Rationale and Aims
• Large scale study in 2013 – 2014
• Context:
• The huge prevalence of the industrial private sector over the public sector
• Old, poorly maintained infrastructure, without sufficient investments
• Geographical reality: vast country, widespread infrastructure, not enough redundancy, few human resources for the protection of sensitive points
• Electricity supply is of vital importance in todays society
• When disrupted, everything associated with the cyber space becomes useless
• It is not possible to put an entire country on backup power generators).
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

It's way too easy to cause a massive blackout in the US

Updated by Brad Plumer on April 14, 2014, 11:00 a.m. ET *@bradplumer* *brad@vox.co*

TWEET SHARE +

The scene at the Capitol building during a blackout. March, 12, 2014 in Washington, DC.

Craig Hudson/For The Washington Post via Getty Im

If you wanted to knock out America's electric infrastructure and leave everyone in t dark for a few weeks, it might not be that difficult.

Assault on California Power Station Raises Alarm on Potential for Terrorism

April Sniper Attack Knocked Out Substation, Raises Concern for Country's Power Grid

Email Print Save 301 Comments A A

By REBECCA SMITH CONNECT

Feb. 4, 2014 10:30 p.m. ET

Shots in the Dark

A look at the April 16 attack on PG&E's Metcalf Transmission Substation

1	2	3	4	5	6	7
12:58 a.m., 1:07 a.m. Attackers cut telephone cables	**1:31 a.m.** Attackers open fire on substation	**1:41 a.m.** First 911 call from power plant operator	**1:45 a.m.** Transformers all over the substation start crashing	**1:50 a.m.** Attack ends and gunmen leave	**1:51 a.m.** Police arrive but can't enter the locked substation	**3:15 a.m.** Utility electrician arrives

Sources: PG&E; Santa Clara County Sheriff's Dept.; California Independent System Operator; California Public Utilities Commission; Google (image)
The Wall Street Journal

Popular Now

ARTICLES

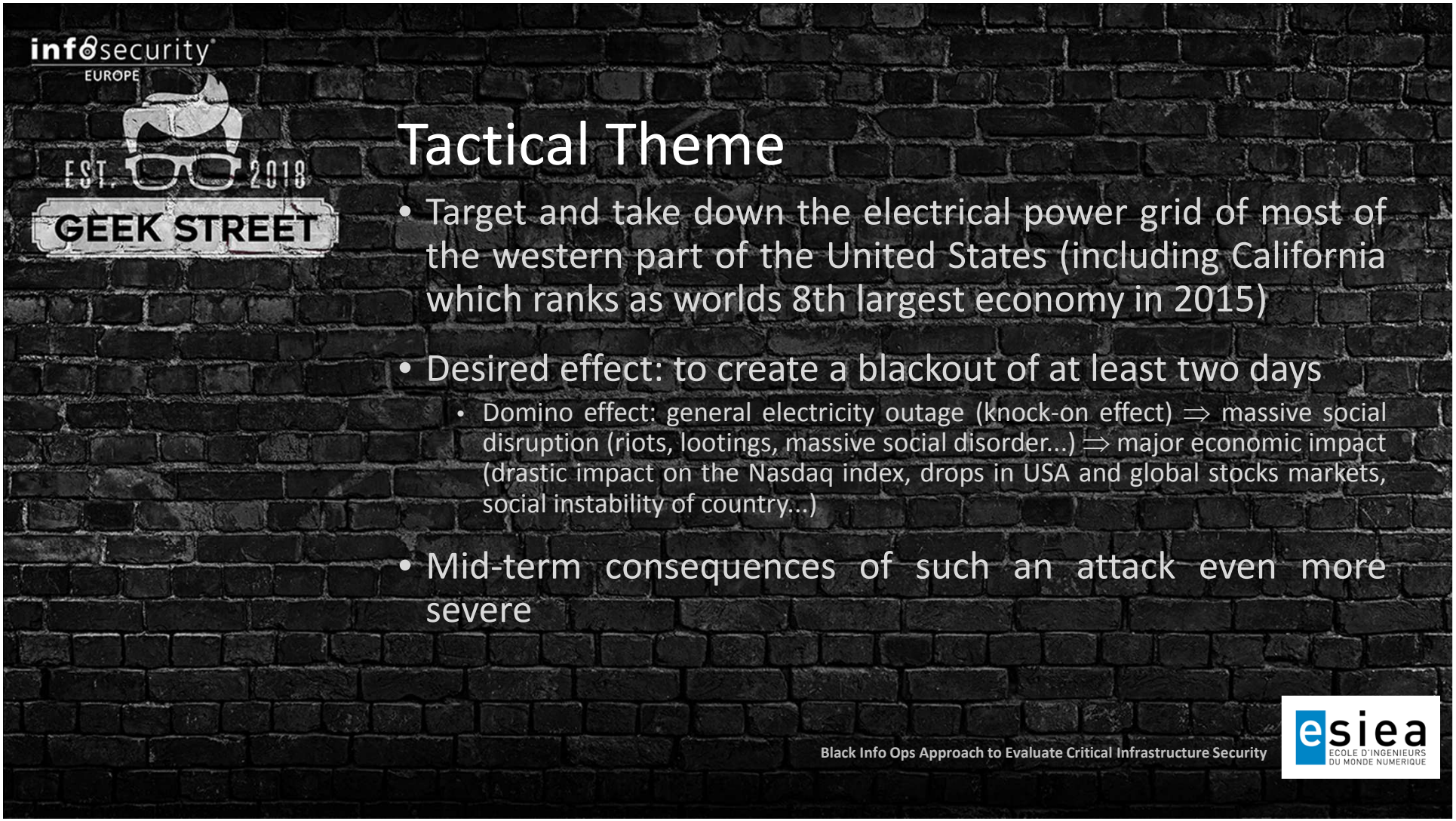
1 Best Places to Find Love

2 Comcast Acquiring Time Warner Cable In All-Stock Deal

3 $2.2 Billion Bird-Scorching Solar Project

4 Assault on Power Grid Raises Alarms

5 BNP Hit by $1.1 Billion Provision


infosecurity
EUROPE
EST. 2018
GEEK STREET
Tactical Theme
• Target and take down the electrical power grid of most of the western part of the United States (including California which ranks as worlds 8th largest economy in 2015)
• Desired effect: to create a blackout of at least two days
• Domino effect: general electricity outage (knock-on effect) ⇒ massive social disruption (riots, lootings, massive social disorder...) ⇒ major economic impact (drastic impact on the Nasdaq index, drops in USA and global stocks markets, social instability of country...)
• Mid-term consequences of such an attack even more severe
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018 GEEK STREET

Intelligence Step

- Full and detailed mapping the U.S. electrical grid (including generating stations, transmission lines, distribution lines, sub-stations). Identification of the sections of the grid which correspond to redundant sources or logistic support between the three main U.S. electrical areas (western, eastern parts and Texas area).
- Geographical problems and constraints.
- Gathering technical data on critical infrastructures such as nuclear plants, especially their external electrical grid or their emergency back-up generators (vital facilities not only to ensure the proper functioning of the nuclear plant but also in case of emergency situations [cooling system]).

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Intelligence Step II

- Collecting and analyzing various types of other openly available data:
  - Road system (identification of the roads which are close to the power infrastructure, and details about special road/traffic regulations around the sites (for example, the vehicle weight and dimension regulations).
  - Sitemap and data on the security system of the infrastructure (monitoring system)
  - Data on Response units (rescue teams, fire-fighters, police, army, national guard…) and also various data such as the number of people working on the spot, the kind of facilities or past incidents recorded from the press for instance.

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018

GEEK STREET

Intelligence Step II (cont.)

- Collecting and analyzing various types of other openly available data:
  - Data on weather conditions and its impact on possible rescue operations ...The time when the attack is launched, is as important as the manoeuver itself. As an illustrative example, attacks that take place in winter or during a heat wave when the electricity consumption is high- will maximize the final effects.
  - Any helpful detail to plan the attack and increase its success probability.

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Intelligence Step III

- All data have been processed to
  - Identify a few tens of relevant facilities (electrical pylons and towers, substations, production plant...)
  - Select the facilities that could be of interest to attackers: spotted areas of difficult access for trucks or helicopters, facilities for which incident detection and repairs are difficult...
  - Draw up a graph which has a sparse and very simple structure due to the nature of the electrical grid.
  - Apply the "Vertex Cover Algorithm" to identify minimal sets of graph nodes to be destroyed in order to get a global impact on the whole graph
- Association rules extraction:
  - *{geographic criteria, climatic criteria, road widths, demographic criteria, equipment, security resources} ⇒ repair time*

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

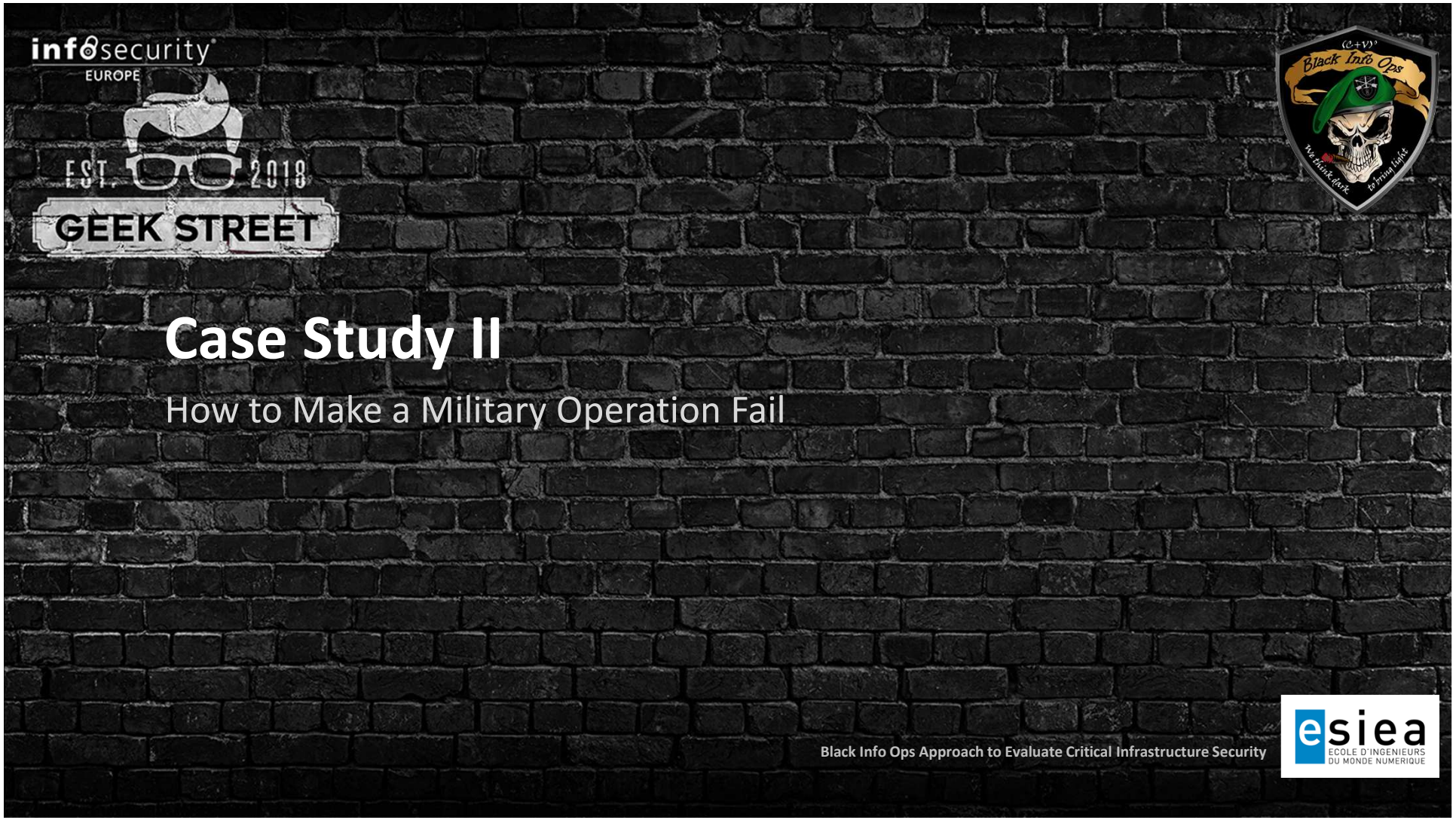
EST. 2018

GEEK STREET

Results and Attack

- We have identified several small sets (vertex cover of about ten nodes) to destroy in order to affect the entire infrastructure
  - The attack step can be carried out by a relatively small group of persons with a light armament.
  - It is even possible to target several sets in parallel while deploying
  - several operational teams on the ground. This enables to maximize the probability of success (operational redundancy) while minimizing operational risks of attack failure

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

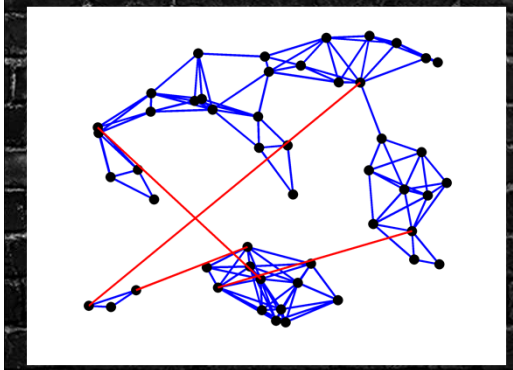

infosecurity
EUROPE
EST. 2018
GEEK STREET
Case Study II
How to Make a Military Operation Fail
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018 GEEK STREET

Rationale and Aims

- Study and simulation conducted in 2008 for the French Navy (published under an "anonymized" version in the National Defence Journal 2009)
  - Show that the bunker approach (e.g. Military port with high security zone) is not valid.
  - Analyze the enlarged version of the target's BCP.
- Tactical theme: delay the departure of an essential battleship for an allied military operation by at least five days. In case of success, the military operation must be cancelled
- Typical case of targets with absolutely no cyber approach angle



(Source: Fu Lin Ph D Thesis 2012)

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018 GEEK STREET

Intelligence Step

- After this step, the following main targets were selected
  - *SUD Huiles*, an oil supplier which obtained the public contract for the Navy
  - *HeliMeca*, a supplier of specific mechanical pieces for the ship and its armament
  - The Navy, due to budgetary difficulties always orders oil and mechanical pieces at the very last moment (at the eleventh hour)
  - *SUD Huiles* and *HeliMeca* have management issues resulting in strong social tension with very virulent unions
  - The delivery of oil can only be made from heavy tonnage trucks and only one direct route (between sea and mountain) is possible, passing through sensitive districts.

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

EST. 2018 GEEK STREET

Course of Events – Event 1

Two main events (many side events, see the 2009 paper). All bricks of attack drawn from real cases.

- Event 1 (as seen by a neutral observer).- A hard strike is triggered in company *SUD Huiles*. Confidential company documents were sent to a major daily newspaper, which evoke a plan of massive redundancies, motivated by heavy losses of the company, due, according to these documents, to embezzlement of funds operated by the plant manager.
- A search by the financial brigade a bit later on in the computers of the company confirms the veracity of these documents. The plant's activity stops.

- Explanation (what the attacker really did)
- Resulting effect: functional failure, the oil is not delivered, the battleship cannot leave

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

Course of events – Event 2

- Event 2 (as seen by a neutral observer).- The day after, clashes between gangs degenerated in sensitive district. They are relatively common in these neighborhoods. Cars blaze, many wounded with knives and an explosive situation monopolizes the attention of the police. The origin of these confrontations seems to come from threats and insults with community and racial characters posted in particular on the site *youtube* and *dailymotion*.
- Tension is gradually rising but the government in place, in an electoral situation, wants to manage the crisis smoothly.
  - Explanation (what the attacker really did)
  - Resulting effect: media diversion, pressure on the political world, variation (second option) by zone control
- Events 1 and 2 seem (and must) appear as uncorrelated

esiea
ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Black Info Ops
Conclusion
Lessons Learned
Key Take Aways
Bibliography
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

infosecurity EUROPE

Lesson Learned

- It is unlikely that pure cyberattacks will represent the sole dimension in future attacks
  - Pure cyberattacks are not sufficient to carry out large-scale attacks successfully to cause significant damage
  - So far, very few successful large-scale cyberattacks on critical infrastructures have been recorded.
  - However, the cyber-dimension proves to be both immensely effective and threatening for the intelligence and planning steps.
- Many other existing large areas of vulnerabilities across the world (critical infrastructure, large companies..). Many interesting and powerful scenarios derived.

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Lesson Learned (2)

- We conclude that economic and political decision-makers do not think globally enough
- No global mapping of functional dependencies with respect to external components
- Less and less resilience
  - Nation States, population, companies are no longer prepared to face extreme conditions
  - This takes part in the self-amplifying properties of the target, which the attackers may rely on

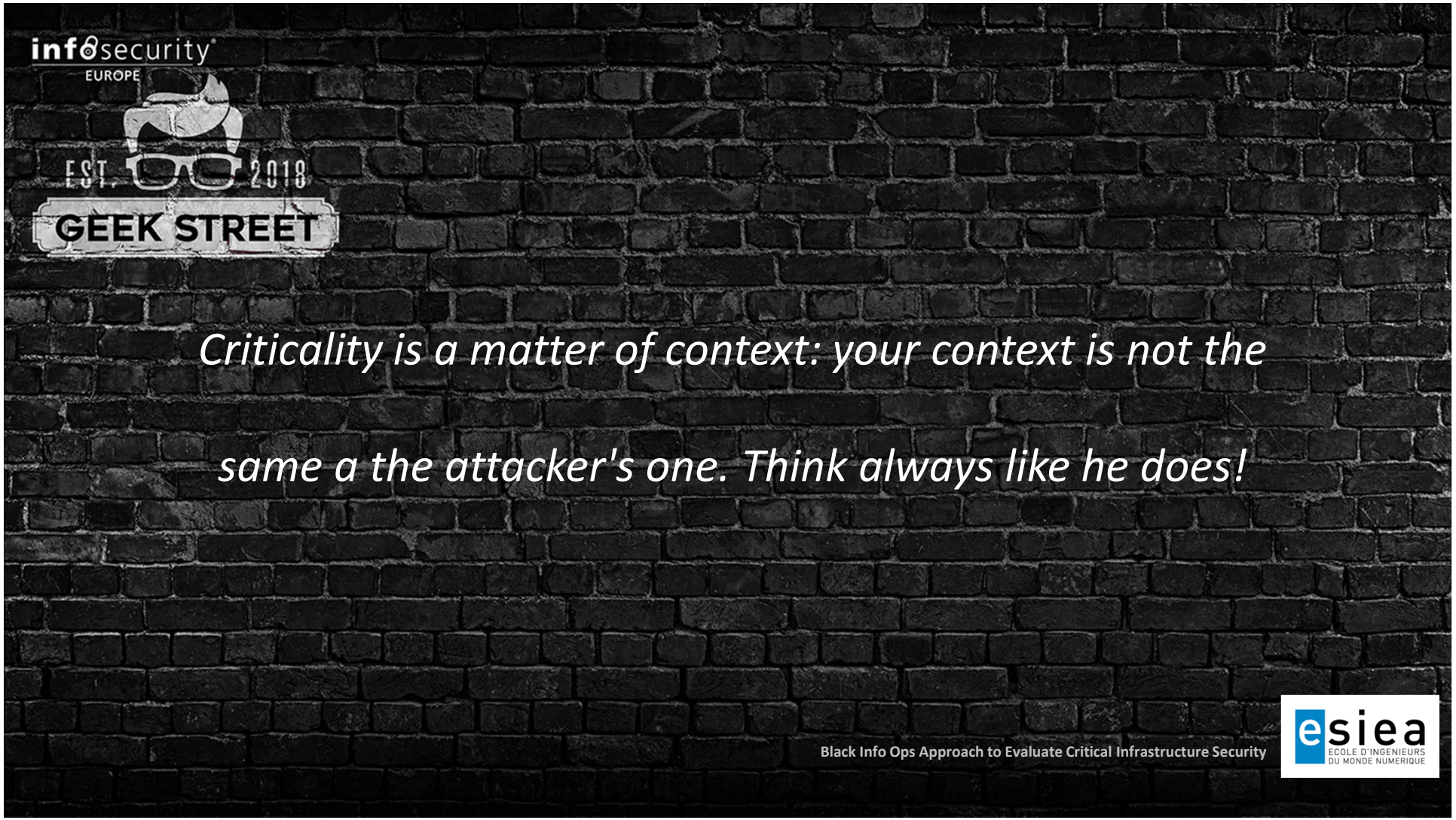
esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

TakeAways

- As a company leader (CEO), to evaluate your actual security
  - If IT and IT security is an important dimension, it is not THE ONLY dimension (you must not see the wood for the trees)
  - Understand FIRST what your business REALLY is, what are its criticality points including your external dependencies
  - You need more a global, functional extended BCP than a simple IT security plan
  - Think in terms of Intelligence and not only in terms of pure technical aspects. The true target are human beings (employees, contractors...) than computers
  - Evaluate your resilience under this enlarges view
- CEO > CSO > CISO > IT Manager
- Criticality is a matter of context: your context is not the same a the attacker's one. Think like he does!

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Criticality is a matter of context: your context is not the
same a the attacker's one. Think always like he does!
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

infosecurity EUROPE

Bibliography

My publications dedicated to these techniques (public studies and analyses only)

- Eric Filiol. *Operational Aspects of a Cyberattack: Intelligence, Planning and Conduct*, in "Cyberwar and Information Warfare", D. Ventre Ed., ISTE, Wiley, 2011
- Eric Filiol. *Operational aspects of Cyberwarfare or Cyber-Terrorist Attacks: What a Truly Devastating Attack Could Do*. In Leading Issues in Information Warfare & Security Research, Vol. 1, pp. 36{53, J. Ryan Ed., Academic Publishing International Ltd, 2011
- Eric Filiol & Gregory Commins. *Unrestricted Warfare versus Western Traditional Warfare: A Comparative Study*. In: Leading Issues in Information Warfare and Security Research, Vol. 2, pp. 73{89, J. Ryan Ed., Academic Publishing International Ltd, 2015

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE

infosecurity EUROPE

Bibliography

My publications dedicated to these techniques (public studies and analyses only)

- Eric Filiol & Cecilia Gallais. *Critical Infrastructure: Where We Stand Today?*. 9th International Conference On Cyber Warfare and Security (ICCWS'2014). Indiana, USA, March 24-25th, 2014, Academic Conferences & Publishing International
- Eric Filiol & Cecilia Gallais. *How Internal and External Dependencies can Affect Infrastructure's Security*. 14th European Conference on Cyber Warfare and Security ECCWS-15, Hateld, UK, July 2-3rd, 2015, Academic Conferences & Publishing International
- Eric Filiol & Cecilia Gallais. *Combinatorial Optimization of Operational (cyber) Attacks Against Large-scale Critical Infrastructures - The Vertex Cover Approach*. 11th International Conference on Cyber Warfare and Security (ICCWS) 2016, Boston, March 17-18th, 2016, Academic Conferences & Publishing International

esiea ECOLE D'INGENIEURS DU MONDE NUMERIQUE


infosecurity
EUROPE
EST. 2018
GEEK STREET
Black Info Ops
Many Thanks for Your Attention
Questions & Answers
filiol@esiea.fr
Black Info Ops Approach to Evaluate Critical Infrastructure Security
esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE