



# MALICIOUS THREATS IN THE VULNERABILITY ANALYSIS OF POWER SYSTEMS

Ettore Bompard

*Politecnico di Torino - Dipartimento di Ingegneria Elettrica*

[ettore.bompard@polito.it](mailto:ettore.bompard@polito.it)

ICNSC Conference

Delft April 12<sup>th</sup> 2011



## OUTLINE

- MALICIOUS THREATS/ATTACKS AND PWRS VULNERABILITY
- NATURE OF MALICIOUS THREATS
- WHY POWER SYSTEMS ARE TARGETS FOR MALICIOUS ATTACKS
- THREATS/ATTACKS TO POWER SYSTEMS
  - TYPES OF THREATS/ATTACKS
  - TARGETS OF MALICIOUS ATTACKS
  - TYPES OF ATTACKERS

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## OUTLINE

- SOME IMPLEMENTED ATTACKS AROUND THE WORLD
- IMPACTS OF THE MALICIOUS ATTACKS
- DEFENSE STRATEGIES
- PRACTICE FROM SOME EUROPEAN SYSTEM OPERATORS
- LEGISLATION AND STANDARDIZATION FOR PREVENTING MALICIOUS ATTACKS
- THEORETICAL APPROACHES FOR MODELING: GAME THEORY (GT) AND MULTI-AGENT SYSTEMS (MAS)
- CONCEPTUAL EXAMPLES

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## .... RUMORS ...

*"... a planned (but prevented) terrorist attack in London, aimed at the heart of the city's electrical power system. The "near disaster" prompted the British government to start a program to look into detail at "critical (energy) infrastructure protection"*

*Stephen Gregory, CEO, Harnser Group, London*

*"The growing vulnerability of the European energy system", Karel Beckman  
European Energy review, 14 March 2011*

ICNSC Conference, Delft April 12<sup>th</sup> 2011



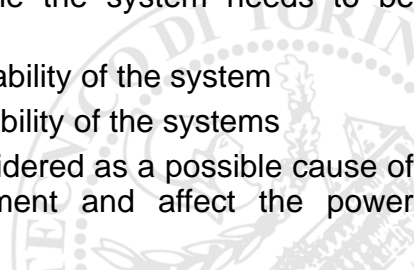
## MALICIOUS THREATS/ ATTACKS AND PWRS VULNERABILITY



## KEY “QUALITIES” AND “ATTRIBUTES” IN PWRS

- **Adequacy:** the ability of the electric system to supply the aggregate electrical demand and energy requirements of the customers at all times in normal operating conditions
- **Security:** the ability to withstand perturbations. It is the availability of (good) reactions to external, abnormal perturbations or natural/accidental and malicious events to keep system feasibility
- **Reliability:** the ability to provide service (supply loads) with high level of probability. To be reliable the system needs to be secure and adequate
- **Robustness:** qualifies the high reliability of the system
- **Vulnerability:** qualifies the low reliability of the systems
- Malicious attacks need to be considered as a possible cause of perturbation in security assessment and affect the power systems vulnerability

ICNSC Conference, Delft April 12<sup>th</sup> 2011





## MALICIOUS THREAT AND ATTACK

- **Malicious threat**: a potential cause of an unwanted incident which may result in jeopardizing a system or an organization; it connotes an initiating event that can cause harm to a system or induce it to fail.
- **Malicious attack**: a set of actions that specifically aim to do harm upon a target system. They are premeditated, with a motivation that can be political (e.g. terrorism), illegal (e.g. organized crime) or just malevolent (e.g. hackers), and executed by threat agents who may be totally external to the system or have internal access to and/or knowledge of the system
- A malicious threat is *potential* while an attacks is *actual* (the implementation of a threat)

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## ANALYSIS OF MALICIOUS THREATS AND ATTACKS

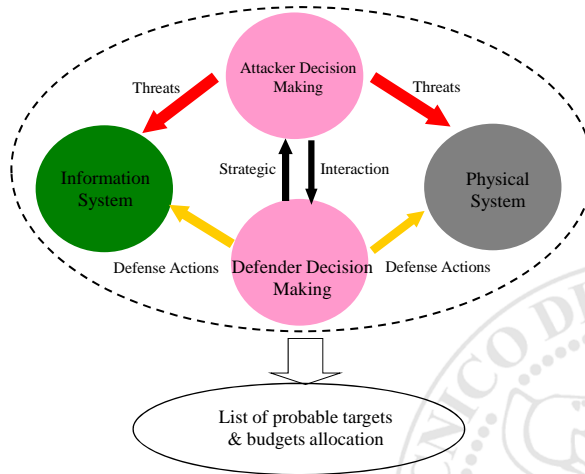
- **Malicious Threats**
  - The analysis of malicious threats is “*off-line*” based on *strategic equilibrium analysis*.
  - “*Preventive approaches*” can be deployed to eliminate threats or shift the focus.
- **Malicious Attacks**
  - The analysis of malicious attacks is “*on-line*” with *dynamic trajectory*.
  - “*Corrective control*” can be deployed to *diminish* damages.

The very **specificity** of malicious threat is in “**preventive**” control while for “corrective” control the “business is as usual”.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



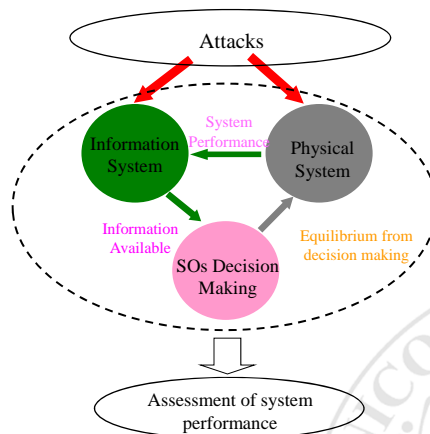
## FRAMEWORK OF THE OFF-LINE SECURITY ANALYSIS



ICNSC Conference, Delft April 12<sup>th</sup> 2011



## FRAMEWORK OF THE ON-LINE SECURITY ANALYSIS



ICNSC Conference, Delft April 12<sup>th</sup> 2011



## NATURE OF MALICIOUS THREATS



## CLASSIFICATION OF THREATS TO PWRs

CAT.	THREAT	DEFINITION
Non-intentional	Natural threats	<i>Natural events not strictly controlled by human that if happen may impact the power system operation causing damages (geomagnetic storms, earthquakes, forest fires, tsunamis, hurricane, flood, lightening, hail, animal, etc.).</i>
	Accidental threats	<i>Possible failure of network devices and the wrong human decisions that may threat power system operation (operational fault, system equipment failure, accident due to the poor management, etc.).</i>
Intentional	Malicious threats	<i>Possibility of intentional actions against power systems facilities and operation, which are undertaken by different agents (terrorist, criminal group, cyber attackers, copper theft, vandal, psychotic, malware writer, etc.) by various means (explosives, high power rifles, malware, etc.) with the willingness to cause damage for getting political or economical benefits.</i>

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## KEY-FEATURES OF MALICIOUS THREATS AND ATTACKS

- An *attack* is the *implementation* of a *threat* and may *cause damages* (economic losses, environmental hazards, social panic, casualties, etc.)
- Are *selective*: the more the target may produce disruptive effects the more it is likely to be attacked
- Are *protection-sensitive*, the tighter the target is protected the less it is likely to be attacked
- The *level of threat*, for a given component, depends on the attitudes, decisions and *interaction between attackers, defenders and sufferers* at a given point in time and space (*strategic interaction*)

ICNSC Conference, Delft April 12<sup>th</sup> 2011



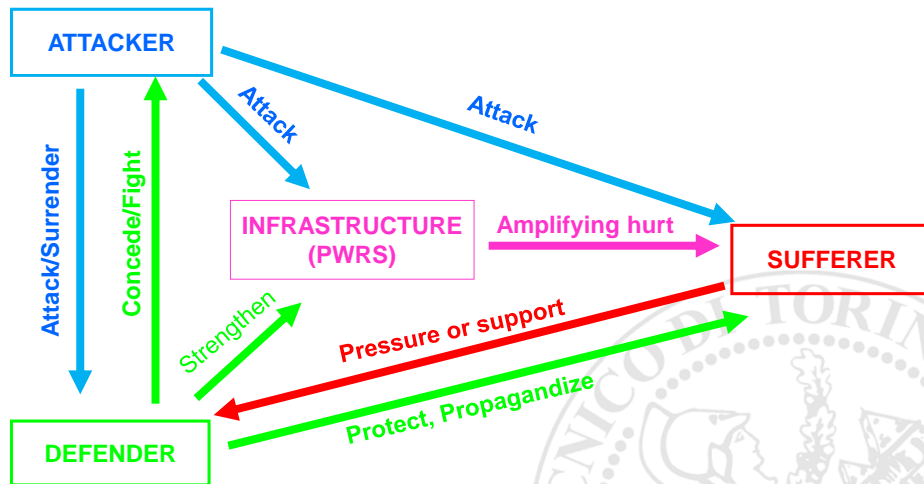
## AGENTS IN MALICIOUS ATTACKS

- *Defender*: public/private organizations and bodies (government, intelligence agencies, police, TSO, GenCos, TranCo, etc.) acting to prevent attacks and maximize, in the long term, system security.
- *Attacker*: malicious agents (terrorists, hackers, intruders, copper thefts, vandals, etc.) deliberately aiming at provoking damages.
- *Sufferer*: stakeholders (people, organizations, companies) that are directly suffered from the attacks and can exert pressures on the defender.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## AGENT INTERPLAY IN MALICIOUS THREATS



ICNSC Conference, Delft April 12<sup>th</sup> 2011



## “DYNAMIC” CONTINGENCY SET FOR MALICIOUS THREATS

- The *strategic interaction* between attackers/defenders /sufferers determines the *probability* of the occurrence of an attack in *time* and *space*.
- Once the most probable attacks have been identified by a *strategic equilibrium analysis*, the possible target is included in the contingency set and protected.
- A malicious threat modifies the *probability distribution* of the contingency. The protection of a target will *shift* the threat to other targets that will be needed to include in the contingency set

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## NATURAL, ACCIDENTAL VS. MALICIOUS THREATS

	<i>Natural Threats</i>	<i>Accidental Threats</i>	<i>Malicious Threats</i>
<b>Motivation</b>	none	accidental	rationaly deliberately
<b>Distribution</b>	random	random	“impacting” component preferred
<b>Risk Assessment</b>	Probabilistic/geo physical approaches	probabilistic approaches	rational interactions models
<b>Counteraction</b>	re-enforce the system	re-enforce the system, training program	re-enforce the system, selective “security”
<b>Strategic Interaction</b>	no	no	yes



## WHY POWER SYSTEMS ARE TARGETS FOR MALICIOUS ATTACKS





## WHY ATTACK PWRs ?

- Large visibility provided by successful attacks (regional/national/continental wide effects).
- Possibility to affect individuals, organizations and businesses in his/her/its activities and interests.
- Huge economic impacts
- Possible “domino effects” due to the physical properties and PWRs structure that may amplify a “properly” chosen action providing large scale impacts.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



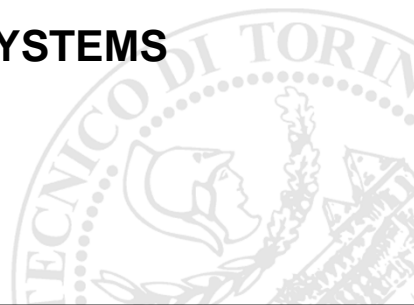
## WHY ATTACK PWRs ?

- Difficulty to protect PWRs due to their large extension and territorial dispersion.
- Diminish civilian morale, forcing a change in the government’s behavior, pressuring them provide advantages to the attackers.
- The loss of power will have a direct impact on the defense structure and the fighting military/police forces rendering the defense system more vulnerable.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



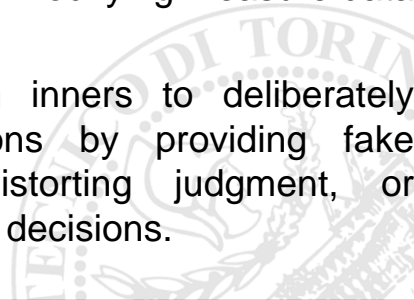
## THREATS/ATTACKS TO POWER SYSTEMS

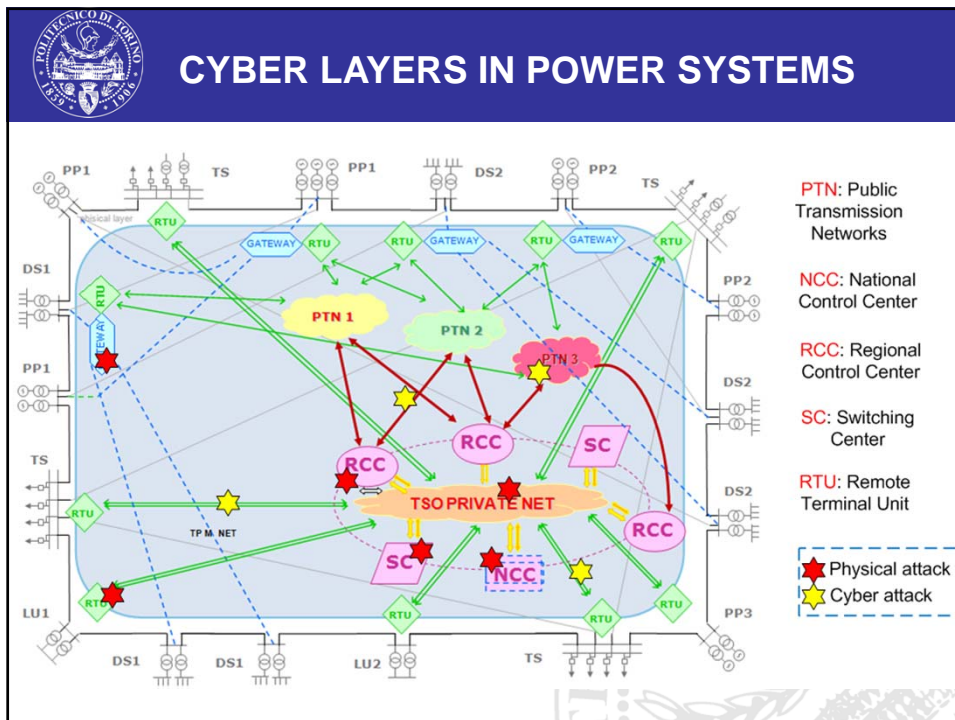
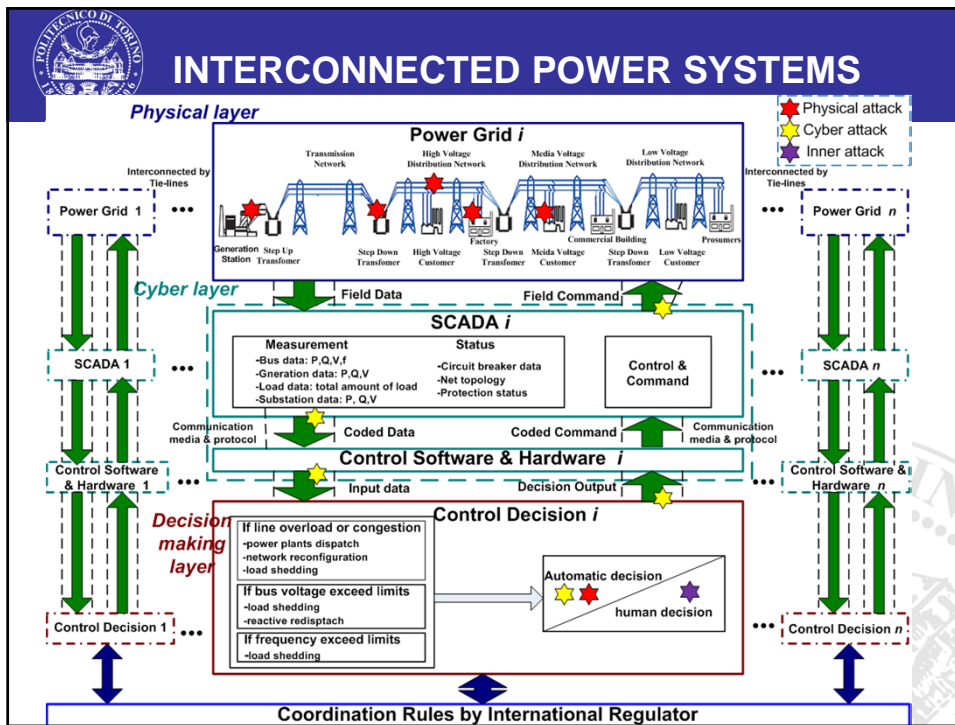


## TYPES OF MALICIOUS THREATS

- *Physical threats*: actions aimed at destroying physical components of the network in both physical and cyber layers.
- *Cyber threats*: actions to incapacitate the communication systems by blocking, delaying, corrupting information flow or modifying measure data or command.
- *Inner threats*: actions from insiders to deliberately facilitate erroneous decisions by providing fake knowledge, intentionally distorting judgment, or premeditatedly mis-executing decisions.

ICNSC Conference, Delft April 12<sup>th</sup> 2011







## TARGETS IN PWRS

TARGETS	ATTACK TYPE
SCADA system	Cyber
PLCs	Cyber
Fault information recorder	Cyber
Sensitive market information	Cyber
Substation host computer	Cyber
Grid control system	Cyber
Overhead line	Physical
Underground cable	Physical
Tower	Physical
Security fence	Physical
Substation (transformer, power cable, circuit breaker, capacitor, relaying and voltage regulators)	Physical
Power plant (generation, power cable, transformer, control center)	Physical
Decision group	Decision

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## TYPES OF ATTACKERS

ATTACKER	DESCRIPTION	ATTACK TYPE
Terrorist	Terrorists seek to destroy power systems facilities to threaten national security and cause mass casualties	Physical & Cyber
Criminal group	They seek to attack/blackmail power systems for monetary gain	Physical & Cyber
Hacker	They break into communication or control to steal information or interferes the normal control operation	Cyber
Insider	The disgruntled insider is a principal source of cyber security.	Cyber
Inner	Deliberately facilitate erroneous decisions	Human decision
Malware writers	Malware designed to damage or disrupt systems	Cyber
Industrial espionage	In order to gain industrial or political advantage	Cyber
Saboteur	The motives for sabotage are frequently rooted in desires for personal, economic, or political gain	Physical & Cyber
Psychotic	Usually as a loner and unlikely to cause widespread grid problem	Physical
Vandal	Vandalism is typically haphazard, random, and relatively localized.	Physical
Copper theft	The theft of copper of power systems on a large scale	Physical
environmental extremist	Try to draw publish attention on environmental concerns	Physical



## SOME IMPLEMENTED ATTACKS AROUND THE WORLD



## ATTACKS IN USA

TIME	SITE	EVENT	ATTACK TYPE	DAMAGE LEVEL
1981	Florida	Two substations were heavily damaged by simultaneous dynamite explosions in one of the most expensive incidents.	Physical	components damage and blackout
1986	Wintersburg, Arizona	Three 500-kV lines from the Palo Verde Nuclear Generating Station were grounded simultaneously over a 30-mile stretch.	Physical	components damage
1987				components damage
July, 1989				components damage
03-2005				actual damage
		electric power grid and had gained access to U.S. utilities' electronic control systems.		
09-12-2010	Fulton, Morrow, Ohio	The thieves cut a hole in the fence and took copper grounding wires, shut off power.	Physical	components damage and blackout
05-02-2011	Valencia county, New Mexico	Copper thieves ripped off Socorro Electric Cooperative, stripping ground wire from poles in the Tierra Grande area.	Physical	components damage

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## EVENTS IN OTHER COUNTRIES

TIME	SITE	EVENT	ATTACK TYPE	DAMAGE LEVEL
30-12-2003	Long quan, zheng ping county, China	Virus spread in the Control system of converter station.	Cyber	No actual damage
26-09-2010	Bushehr, Iran	30,000 industrial computer systems of the nuclear reactor project of Iranian Bushehr Nuclear Power Plant had been infected by the Stuxnet virus. <a href="#">The first-known cyber attack targeted at power systems.</a>	Cyber	No actual damage
2002		Cigre conducted an international study of power substation security. Out of their 40 respondents 35 reported that they had at least one unauthorized intrusion annually.	Physical	
10-07-2003	Corrs Corner, Northern Ireland, UK	A substation has been attacked a number of times during the last two months by vandals throwing stones at electricity equipment on the site. It had resulted in damage to equipment installed in the high voltage substation.	Physical	components damage
16-03-2004	Mosca, RUS	Bomb against electric lines tower.	Physical	components damage
15-09-2004	Irun, ES	Bomb against high voltage tower.	Physical	components damage

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## EVENTS IN OTHER COUNTRIES

TIME	SITE	EVENT	ATTACK TYPE	DAMAGE LEVEL
30-08-2004	Baghdad, IRQ	Explosion of three car bombs during the ceremony for the inauguration of a water plant (42 dead, 140 wounded).	Physical	Death of staff and components damage
2005	Qinghai province, China	According to the statistics, in 2005, 137.11 km cable, 15 transformer, 60 solar panels and 3840 steel blocks of tower are stolen.	Physical	
05-01-2006	Sos del Rey Catolico, ES	Bombs against a hotel and an electric substation.	Physical	components damage
07-01-2006	Jaca, ES	Bomb against a power plant	Physical	components damage
02-03-2006	Nahrwan, IRQ	Malicious attacks against a power plant (9 dead, 2 wounded)	Physical	Death of staff and components damage
20-03-2006	Baiji, IRQ	Attacks against three engineers of a city power plant (3 dead)	Physical	Death of staff and components damage
24-03-2006	Taji, IRQ	Attacks against three engineers of a power plant (3 dead)	Physical	Death of staff and components damage
10-05-2006	Ba'qubah, IRQ	Bomb against some officers of an electric company (5 dead, 6 wounded)	Physical	Death of staff and components damage
01-08-2006	Baghdad, IRQ	Attacks against a minibus of officers of the power plant (3 dead, 6 wounded)	Physical	Death of staff and components damage

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## EVENTS IN OTHER COUNTRIES

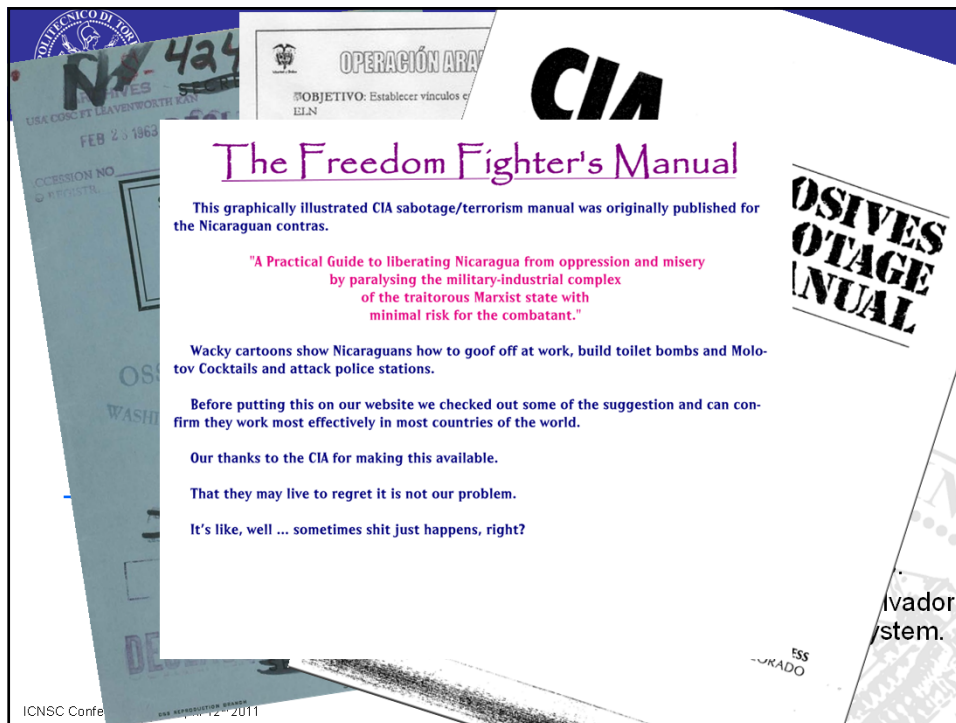
TIME	SITE	EVENT	ATTACK TYPE	DAMAGE LEVEL
09-10-2008	Elizabeth Downs, Adelaide, Australia	Offenders broke into a high-voltage substation and stole valuable copper wiring. Blackouts spread from Elizabeth and Gawler, into the Adelaide Hills and as far south as Kilburn .	Physical	components damage and blackout
20-07-2009	The area of South East London and North Kent, UK	The vandals deliberately caused a fire near a cable installation, which caused failure of a 132 kV cable and four circuit boards. As a result, power supplies were cut to around half of the homes for around 4 days, whilst other homes were given 3 hour allocations of power followed by 6 hours "off" .	Physical	components damage and blackout
03-05-2010	Bolton, Greater Manchester UK	An electrical surge caused by copper thieves led to a power cut for almost 400 properties in Bolton.	Physical	components damage and blackout
12-07-2010	Ronchin, France	Four copper thieves stole 1.86 miles of electric cables which made 118 trains delayed.	Physical	components damage and trains delayed


ICNSC Conference, Delft April 12<sup>th</sup> 2011



## IMPACTS OF THE MALICIOUS ATTACKS





 **IMPACT OF MALICIOUS ATTACKS**

- A large set of impacts are shared with natural and malicious threats and may assessed with the same metrics (loss of power supply, cost of equipment damage, outage duration, casualty, environmental hazards, direct monetary loss, total monetary loss)
- Specific impacts are mainly related to the physiological impacts on the population (feelings of vulnerability, distrust in the Institutions) and possible change in the state policy due to the pressures exerted through the attacks
- Increase in the protection cost of the infrastructure with increase in the electricity cost and reduction in market efficiency

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## PERSIVED IMPACTS ON THE POPULATION

- **Transportation:** trains, subways, street lights, and air traffic will all be jammed or stopped.
- **Emergency services:** hospitals will be forced to use backup power. Police and fire department responses will be longer.
- **Public utilities:** water, gas, and sewer services will be interrupted, eventually causing health problems.
- **Industrial:** manufacturing will stop across-the-board until power is restored (unless the plant has its own generating facility). In addition, losses may occur in sensitive processes such as steel manufacturing because of the sudden loss of power.
- **Computers and telecommunications:** the loss of power will interrupt computer operations and may result in the loss of data or other damage. Depending on the availability of emergency power, telecommunications will also be affected.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## COSTS DUE TO THE BLACKOUT

PRIMARY USER	DIRECT COST COMPONENTS	INDIERCT RESTS	REMARKS
Residential	<ul style="list-style-type: none"> <li>a. Inconvenience, lost leisure, stress</li> <li>b. Out-of-pocket costs such as spoilage and property damage</li> <li>c. Health and safety</li> </ul>	<ul style="list-style-type: none"> <li>a. Costs on other households and firms</li> <li>b. Cancellation of activities</li> <li>c. Looting or vandalism</li> </ul>	Indirect costs are a minimal, if not negligible, fraction of total (direct and indirect) costs of a curtailment
Industrial, commercial and agricultural firms	<ul style="list-style-type: none"> <li>a. Opportunity costs of idle resources such as labor, land, capital, profits</li> <li>b. Shutdown and restart costs</li> <li>c. Spoilage and damage</li> <li>d. Health and safety effects</li> </ul>	<ul style="list-style-type: none"> <li>a. Cost on other firms that are supplied by impacted firms (multiplier effect)</li> <li>b. Costs on consumers if impacted firm supplies a final good</li> <li>c. Health and safety-related externalities</li> </ul>	Indirect effects are likely to be minimal for most capacity-related interruptions, but can be significant component of total costs for longer duration energy shortfalls.
Infrastructure and public service	<ul style="list-style-type: none"> <li>a. Opportunity cost of idle resources</li> <li>b. Spoilage and damage</li> </ul>	<ul style="list-style-type: none"> <li>a. Costs to public users of impacted services and institutions</li> <li>b. Health and safety effects</li> <li>c. Potential for social costs stemming from looting and vandalism</li> </ul>	Indirect costs constitute a major portion of total costs of curtailment

SOURCE: Office of Technology Assessment, US Congress

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## EXAMPLE: COSTS OF THE NORTHEASTERN BLACKOUT 2003

Approximate Start Time	Approximate End Time	Lost Megawatt MW	Duration Hour	MWh	Cost (\$ Billion)	
					Lower Bound	Upper Bound
8/14 – 4 PM	8/14 – 8 PM	61,800	4	247,200	\$1.8	\$2.8
8/14 – 8 PM	8/15 – 6 AM	30,900	10	309,000	\$2.3	\$3.4
8/15 – 6 AM	8/15 – 10 AM	15,450	4	61,800	\$0.5	\$0.7
8/15 – 10 AM	8/16 – 0 AM	13,200	14	184,800	\$1.4	\$2.1
8/16 – 0 AM	8/16 – 10 AM	6,600	10	66,000	\$0.5	\$0.7
8/16 – 10 AM	8/17 – 6 AM	2,000	20	40,000	\$0.3	\$0.4
8/17 – 6 AM	8/17 – 4 PM	1,000	10	10,000	\$0.1	\$0.1
<b>Total Economic Cost</b>					<b>\$6.8</b>	<b>\$10.3</b>

SOURCE: ICF Consulting

*Shocked* by the accidental blackout? What if a blackout *provoked* by *malicious attacks*?

Failure caused by *random events* from the nature could breed such *wreak havoc* on the economy. Can we *imagine how severe* the *devastating damage* and *how many times* of *costs* it would trigger from *an elaborately designed* attack?

10? 100? Or **More?**

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## DEFENSE STRATEGIES



## GENERAL SECURITY POLICY

- Include in the security policies at various levels (governmental, police, TSOs and utilities) special considerations of malicious threats/attacks.
- A list of general policies related to malicious attacks:
  - **Responsibility**: Staff for general, physical, cyber security should be clearly aware of the separately and appropriately predefined duties of their own.
  - **Rules**: Guidance for security practice, including inspections and reliability tests, etc.
  - **Training**: Programs to enhance the recognition for general and security staff of their responsibility and corresponding rules.
  - **Self-Assessments**: evaluation of the state of the security program and each individual staff.
  - **Emergency Plans**: quick response processes and plans for corrective control after attacks, aiming at maximizing maintaining the functionality of the system as well as possibly limiting the damage.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## GENERAL REDUCTION OF VULNERABILITY

- Making security as a **design parameter** in PWRS could guide the evolution of future systems toward inherently less vulnerable technologies and configurations.
- **Emphasize** inherently less vulnerable technologies and designs where practical, including pole-type transmission lines, underground transmission cables, and standardized equipment.
- **Move toward** an inherently less vulnerable bulk power system (e.g., smaller generators near loads) as new facilities are planned and constructed (“smart grids”).

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## PREVENTING DAMAGES

- **Harden** key substations-protect critical equipment within walls or below grade, **separate** key pieces of equipment such as transformers, **reinforce** the equipment itself to resist damage, etc.
- **Surveillance** (remote monitoring) around key facilities (coupled with rapid-response forces).
- Maintain **guards** at key substations.
- Improve **coordination** with law enforcement agencies to provide threat information and coordinate responses.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## LIMITING CONSEQUENCES

- Improve emergency procedures for handling power flow instability after major disasters and ensure that operators are trained to implement these contingency plans.
- Modify the physical system-improve control centers and protective devices, greater redundancy of key equipment, increased reserve margin, etc.
- Increase and re-locate spinning reserves.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## SPEEDING RECOVERY

- Contingency planning for restoration of service, including identification of potential spares and resolution of legal uncertainties.
- Clarify Legal/institutional framework for sharing reserve equipment.
- Stockpile critical equipment (transformers) or any specialized material (e.g., various types of copper wire) needed to manufacture this equipment.
- Assure availability of adequate transportation for a stockpile of very heavy equipment by maintaining database or rail/barge equipment and adapting Schnabel cars to fit all transformers if necessary.
- Monitor domestic manufacturing capability to assure adequate repair and manufacture of key equipment in times of emergency.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## PRACTICE FROM SOME EUROPEAN SYSTEM OPERATORS





## TSO 1 (NORTHERN EUROPE)

- **PLANNING**
  - Network planning principles (N-1) in power system, redundant capacity
  - Planning guidelines of substations, transmission lines, ITC – systems
  - Contingency planning including loss of control room and ITC facilities training
  - Dispatching, fault detection and power recovery training, simulator training
  - security training,, crisis management exercises, fire and rescue skills
- **PERIMETER SECURITY**
  - fences, gates etc
  - alarm systems (control rooms, perimeter alarm systems)
  - CCTV (for major substations)
  - access control (major substations)
  - transformer bunkers on 400/110 kV transformer
- **CO-OPERATION**
  - co-operation with Defense forces in planning an practicing of critical nodes
  - chance of information with Security Police & other companies
- **MATERIAL**
  - pylon material to replace quickly broken transmission line pylons (catastrophe)

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## TSO 2 (SOUTHERN EUROPE)

- **Buildings**
  - In the Control Centers there is a double wicket with an intermediate space. There are cameras looking at this intermediate space, and the monitoring is handled by a guard, who is responsible for the incoming and outgoing vehicles through the main entrance.
  - Magnetic cards are used in order to check the entrance of individuals inside the building. These cards have been given only to the authorized staff.
  - Each Control Center has a generating machine and batteries, in case of a partial or a whole black out, for the uninterrupted operation of the Control Center.
- **Operational security**
  - The National Control Center has a consecutive cooperation and direct phone line to the Security Ministry.
  - A firewall protects the Information System, the SCADA and the intranet of the TSO. Only the authorized staff has access to the above networks.
  - In the future plans of the TSO is the installation of a backup SCADA for increased security.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## TSO 4 (EASTERN EUROPE)

- **Physical security program**
  - Each facility will be provided with an integrated security system, including CCTV, control access, anti-burglary system, perimeter detection system
- **Cyber security program**
  - Specific actions concerning different aspects of cyber security
  - The standard ISO 17799 is implemented for certain processes
- **Acknowledge people within the electricity sector and within state entities**
  - 2 major events in 2005 and 2006
- **Raise cooperation within the electricity sector**
  - Working group was established within the Ministry of Economy and Commerce

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## TSO 5 (CENTRAL EUROPE)

- **Organizational measures**
  - Definition of the ways of communication in a company guideline
  - Implementation of an emergency-protection organization
    - crisis management group (in the headquarter and in the operational branches)
    - emergency-protection manager in the headquarter
    - emergency-protection manager in each operational branch
  - Provision of an emergency-protection guideline (responsibilities, processes, documents, communication)
  - frequent training of the emergency-protection team
- **Tasks of the crisis management group in the headquarter**
  - to analyze incidents and their progression
  - to assess the current state
  - to develop a strategic plan of action
  - to decide
  - to lead crisis communication
  - to inform enterprise headquarter, associated bodies of supervision, public authorities, employees
  - to guide through the crisis

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## TSO 6 (SOUTHERN EUROPE)

- **The n-1 Redundancy Rule is kept**
- **Power Stations**
  - On-Site Police Guard
  - CCTV Perimeter Surveillance
  - Anti-Intruder Perimeter Protection
  - Quick Police Reinforcements
  - Access Control
- **The NECC**
  - On-Site Police Guard
  - CCTV Surveillance System
  - Access Control System
  - Emergency NECC at another location
- **Substation**
  - Fenced and Securely Locked
  - Frequently Inspected

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## LEGISLATION AND STANDARDS FOR PREVENTING MALICIOUS ATTACKS





## LEGISLATION

NATION	TITLE	DATE	CONTENTS
USA	The Grid Reliability and Infrastructure Defense Act	June 9, 2010	The "GRID Act" would amend the Federal Power Act to issue emergency orders requiring critical infrastructure facility operators to take actions necessary to protect the bulk power system .
USA	The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets	February, 2003	This act provided a statement of national policy to remain committed to protecting critical infrastructures and key assets from physical attacks.
EU	Directive CIP critical infrastructure protection European critical infrastructure		The new directive will also supersede a 2005 Council framework decision on cybercrime, because that previous regulation did not focus sufficiently on evolving threats - in particular, large-scale simultaneous attacks against information systems.
China	Electricity Law of the People's Republic of China	December 28, 1995	In this law, the chapter VII named "Protection of Power Facilities" has defined the behavior of malicious attacks to power facilities, and provided the corresponding penalties.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## STANDARDS

ABBREVIATION	TITLE
IEEE 1402	IEEE Guide for Electric Power Substation Physical and Electronic Security
IEC 62210	Initial Report from IEC TC 57 ad-hoc WG06 on Data and Communication Security
IEC 62351	Data and Communication Security
NERC 1200	Urgent Action Standard 1200 – Cyber Security
NERC 1300	Cyber Security, also known as CIP-002-1 through CIP-009-1
NERC Security Guidelines	Security Guidelines for the Electricity Sector
FERC SSEMP	Security Standards for Electric Market Participants
ISA SP99	Manufacturing and Control System Security Standard
NIST PCSRF	Security Capability Profile for Industrial Control Systems
ISO 15408	Common Criteria for Information Technology Security Evaluation
ISO 17799	Information Technology – Code of practice for information security management

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## THEORETICAL APPROACHES FOR MODELING MALICIOUS THREATS: GAME THEORY (GT) AND MULTI-AGENT SYSTEMS (MAS)

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## GAME THEORY (GT) APPLICATIONS

- Game theory is concerned with the actions of decision makers who are conscious that the actions of the other game participants affect their utility.
- Game theory is suitable for modeling the interaction between attackers and defenders that take place in a context in which each player's behavior impacts the achievement of the goals of all other players in the game.
- Game theory in PS can address the issue of pointing out which point and/or component has higher probability to be attacked.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## MIXED STRATEGY GAME FOR RANKING POWER SYSTEM COMPONENTS

- A *mixed strategy* of a player in a game is a probability distribution over the player's actions.
- Define the system components (line/substation) to form the meaningful the '*failure set*' or '*attacking action set*'.
- For each attack, the system is analyzed in the new status and the consequences evaluated in terms of *payoffs* of the defender and attacker to form a payoff matrix.
- The *mixed strategy equilibrium* provides the probability of each component to be attacked and consequently the related risk.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## EQUILIBRIUM EVALUATION FOR OFF-LINE ANALYSIS

- The interaction of the various entities in the analysis is studied under the hypothesis of rational player.
- The rationality player hypothesis implies that each entity or player will act to maximize his/her own utility.
- An equilibrium is a situation in which no player has interest to change his/her decision if the other players don't change theirs.
- Equilibrium is the outcome sought in the modeling process and that allows for the evaluation of the possible actions and the related probabilities.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



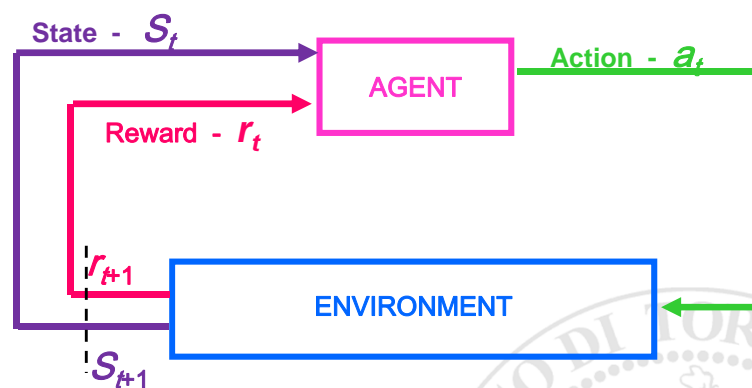
## MULTI-AGENT SYSTEMS (MAS)

- An *agent* is an abstract or physical autonomous entity which performs a given task using information gleaned from its environment to act in a suitable manner so as to maximize a given measure of its utility.
- The agent should be able to adapt itself based on changes occurring in its environment, so that a change in circumstances will still yield the intended result.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## INTERACTION BETWEEN AGENT AND ENVIRONMENT



At each time step  $t$ , the agent senses the current state  $s_t = s \in S$  of its environment and on that basis selects an action  $a_t = a \in A$ . As a result of its action, the agent receives an immediate reward  $r_{t+1}$ , and the environment's state changes to the new state  $s_{t+1} = s' \in S$ .

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## DEFINITIONS IN MAS

- **Agent:** may be *attacker* (terrorists, hackers, intruders, insiders, etc), *defender* (government, police, intelligence agencies, TSOs, GenCos, etc), *sufferer* (individuals, companies, society, ecology, etc).
- **Environment:** *outside situation* network status, defence force deployment, actions in place, etc.
- **State:** *collective information* contained in the environment at time  $t$ , such as attacks happened and are happening, current defence actions, available resources, sufferers' pressures, etc.
- **Action:** *chosen strategy* at time  $t$  to *maximise* agents' own utility, considering the environment and its state, such as where and how to attack, allocations for defence resources, etc.
- **Reward:** *contributions* to the *individual utility* of an agent from the environment after taking some actions, such as caused damages for attackers, diminished costs for defenders, etc.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## CONCEPTUAL EXAMPLES

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## SYSTEM COMPONENTS RANKING W.R.T THE RISK/PROBABILITY TO BE ATTACKED

- **Objective** → attribute to each system component a probability of attack and provide a ranking of the components according to the probability/risk of an attack.
- **Theory** → game theory application.
- **Framework** → a PS is considered in which one attacker (terrorist organization) may be willing to attack the bus substation (cut off all connected lines) and only one organization is in charge to defend it (TSO).
- **Model features** → GT model based on mixed strategies game which equilibrium (MSE) provides the set of probability of an attack for each bus.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## MIXED STRATEGY EQUILIBRIA INPUT

Line information							
Line No.	From Bus	To Bus	X.V.	Flow Limit(MW)	Att. Cand.	Attack cost (k€)	Protect Cost (k€)
1	2	1	0.0575	400	0	15	21
...	...	...	...	...	...	...	...

Node information							
Node Name	Power (MW)	Power Min(MW)	Power Max(MW)	Node Sta	Att. Candi.	Attack Cost (k€)	Protect Cost (k€)
1	203.4	-240	0	1	1	60	50
...	...	...	...	...	...	...	...

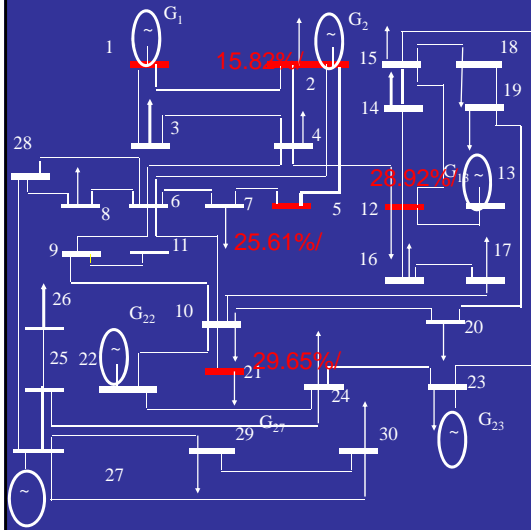
Parameter		
MultiAttack	Power Alloc. Type	Beta
1	2	0.2

*The completely destroyed probability of the attacked component, once it is protected*

1. Minimize the line flow variation
2. Minimize the node power variation



## MIXED STRATEGIES EQUILIBRIA IEEE30-BUS TEST SYSTEM



Attacks	Bus	Probability	Risk(M€)
1	0	0	0
2	1	0	0
3	2	15.82%	35.26
4	5	25.61%	57.14
5	12	28.92%	64.52
6	21	29.65%	66.15



## IMPACTS EVALUATION OF THE COORDINATION AND COMMUNICATION

- **Objective** → assess the impact of coordination and communication in power system.
- **Theory** → multi-agent system with Q-learning approach for the agents.
- **Framework** → the network is operated by three TSOs, they may be coordinative / independent, communicating / non-communicating.
- **Model features** → MAS to simulate the real system operation by the agent learning and find out the exact outcome of different operation scenarios.



## INDIVIDUAL & SOCIAL RATIONALITY

- Individually rational agent: focuses only on its own (individual) utility when deciding which action to take;
- Socially rational agent: also considers the utility of other agents when deciding which action to take;
- Expected utility of the agent (EU): generally is composed by two terms:

$$EU(\alpha) = f(IU(\alpha), SU(\alpha))$$

$IU \rightarrow$  individual utility ,  $SU \rightarrow$  social utility,  $\alpha \rightarrow$  action

Utility in this context means the evaluation of the action implemented by the agent.

- Action Set: each agent can shed the loads at some buses in its local subsystem.



## CALCULATION OF UTILITY

- For actions that can not remove congestions completely, the action causing less overloaded rate should have higher utility.

Utility = Total Overloaded Rate (negative)

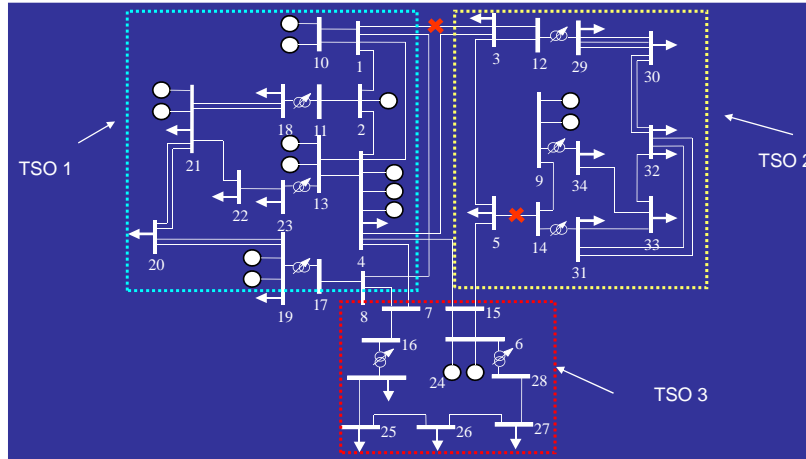
- For actions that can remove congestions completely, the action shedding less loads should have higher utility.

Utility = M – Quantity of total shed loads (positive)

(M is a constant which must be bigger than maximum possible quantity of total shed loads in one action.)



### 3 TSOs EXAMPLE

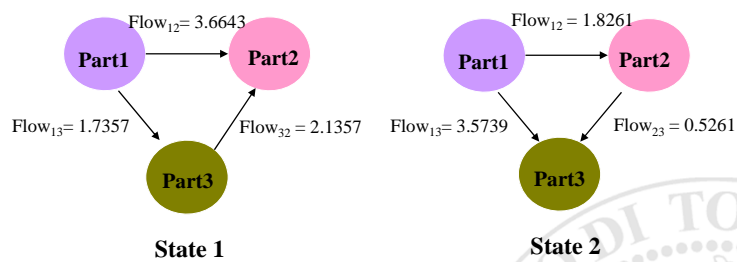


✱ POSSIBLE ATTACKS

ICNSC Conference, Delft April 12<sup>th</sup> 2011



### SYSTEM STATES CONSIDERED



ICNSC Conference, Delft April 12<sup>th</sup> 2011



## COMMUNICATIONS IMPACTS FOR INTERCONNECTED SYSTEMS (STATE 1)

	NO COMMUNICATIONS Individually rational agents			COMMUNICATION Socially rational agents		
	TSO 1	TSO 2	TSO 3	TSO 1	TSO 2	TSO 3
	Bus of shed loads	None	33 34	None	None	33 34
Utility	20	18.8	20	20	18.8	20

Individually rational agents converge in 435,856 iterations and socially rational agents converge in 423,393 iterations.

- For state 1, both locally rational agents and socially rational agents can find the same actions to remove all security congestions.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## COMMUNICATIONS IMPACTS FOR INTERCONNECTED SYSTEMS (STATE 2)

	NO COMMUNICATIONS Individually rational agents			COMMUNICATION Socially rational agents		
	TSO 1	TSO 2	TSO 3	TSO 1	TSO 2	TSO 3
	Bus of shed loads	23	3 5	7 27	23	3 5
Utility	19.4	-0.1655	19.1	19.4	17.2	18.9

Individually rational agents converge in 435,856 iterations and socially rational agents converge in 423,393 iterations.

- At state 2, agent 2 may not have enough sources to remove the security congestions in its local system by itself. When communication is not available, agent 1 and agent 3 can not get the information about the security situation of agent 2 and help it to remove its security congestion.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## COORDINATION IMPACTS

	Coordination		Independence	
	Power Generated [pu]	Loads Supplied [pu]	Power Generated [pu]	Loads Supplied [pu]
TSO 1	9.05	7.05	7.65	7.65
TSO 2	2.9	1.9	1.55	1.55
TSO 3	0	3	1.5	1.5
Total	11.95	11.95	10.7	10.7

- From the overall perspective, coordination should be better than independence.
- Agent 2 and agent 3 would like to choose coordination because more loads in their subsystems will be supplied. But agent 1 would not. To persuade agent 1 to coordinate, agent 2 and agent 3 may wish to pay some compensation.



## CONCLUSIONS

- *Malicious threat* may have *disastrous impacts* on power systems and society *far heavier* than “traditional” black-outs due to the possible “good design” of the planned failure;
- The *cost to prevent* malicious threats and attacks is *huge* for an event for which the *risk* is *hardly possible* to be precisely *assessed* and can *drastically vary* over time due to the *constantly changing* international *social/political environment*.
- The *implementation* of defense strategies *takes time* and *cannot* be *turned on* only as a consequence of an uprising level of alarm.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## CONCLUSIONS

- The *implementation* of defence is *imperative* and *cannot* be imposed and recovered only on a *monetary basis*.
- The *security level* and corresponding *investment* need to be strictly *regulated* and *normalized* by the regulator proving the right mechanism for *collecting* the resources and *pricing* security properly.
- Malicious threats are *inherently different* from natural/accidental threats; thus proper models for *vulnerability assessment* are needed.

ICNSC Conference, Delft April 12<sup>th</sup> 2011



## CONCLUSIONS

- *Game theory* is able to describe the *interaction* between the *defender* and *attacker* so as to *rank* the *risk* of the power system components and provide an effective way of *assessing* the system *vulnerability*.
- *Multi-agent system* is capable of *simulating* the *system operation* under different scenarios to *discover* the *weakness* of the system operation.

ICNSC Conference, Delft April 12<sup>th</sup> 2011