HUMAN FACTORS IN CYBERSECURITY FOR TRANSPORTATION SYSTEMS

JEAN CAIRE
Department of Safety Control, RATP, Paris, France

ABSTRACT

Railway systems follow the same trend than the other transportation modes, namely the integration of IT into all functional areas of operations that created both opportunities and vulnerabilities. In the same time, Cyber-crimes are on the rise and several companies have already experienced successful or attempted attack against their industrial control systems for reasons as diverse as sabotage or blackmail and extortion, while several state actors are developing offensive cyber operations programs that could one day target critical infrastructures. To address these challenges, RATP has developed a structured approach for security assessment, encompassing physical, cyber and human realms that highlighted the specific threat posed by Insiders.

Keywords: AUGT, cyber-attack, insiders, spectrum of influence, manipulation.

1 INTRODUCTION

We are witnessing a fast-growing development of state doctrines with respect to offensive cyber operations likely to be used against critical infrastructures, now considered as high value targets. For instance, the disruption of railway transport or even the derailment of trains are part of the possible effects delivered by a cyber-attack according to US strategists. From a practical point of view, cyber-crimes are on the rise and several companies have already experienced successful or attempted attack against their industrial control systems for reasons as diverse as sabotage or blackmail and extortion. Furthermore, railway systems follow the same trend than the other transportation modes, namely the integration of IT into all functional areas of operations that created both opportunities and vulnerabilities.

In that context, RATP is currently developing a structured approach for security assessment, encompassing physical, cyber and human realms.

We present a general framework for the study of the cyber threat that insiders (i.e. employees who wittingly or unwittingly commit or facilitate the commission of a malevolent action) pose to Automated Urban Guided Transport (AUGT).

2 MODEL OF OFFENSIVE CYBER-OPERATIONS

As the raising number of cases reveals, cyberspace has become a place of confrontation and. critical infrastructures like urban AUGT are becoming high value targets for a large set of Adversaries.

A cyber-attack, or more accurately an offensive cyber operation, is a projection of power in cyberspace or, through it, towards physical and human entities [1].

2.1 Potential effects of cyber-attacks

One could undertake an offensive cyber-operation against a critical infrastructure for two reasons [2]:

- deny the use of the infrastructure to its operator;
- exploit the infrastructure's services to improve its own capabilities.

Thus, offensive cyber operations can achieve a wide array of effects (Fig. 1).

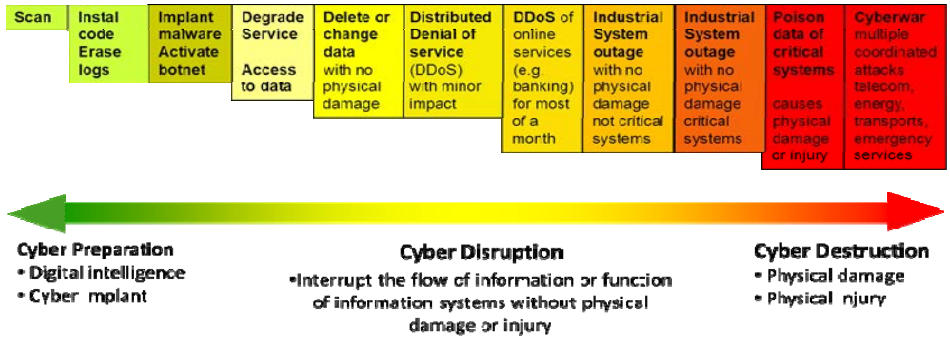

Figure 1: Spectrum of offensive cyber-operations (adapted from [3]).

2.2 Threat actors and vectors

We categorize cyber threats through the technical capabilities necessary to exploit the vulnerabilities of a targeted system [4]:

- *Remote access without user assistance* targets system-level processes on a machine;
- *User-assisted remote access* targets common applications;
- *Close access* permits an attacker to copy and execute malware onto a machine through routine operation;
- *Insider access* is the unauthorized manipulation of the targeted system by individuals with legitimate access;
- *Outsourced service* is the access to systems through individuals or companies contracted to provide services to the target;
- *Supply chain access* refers to embedding malicious logic, software or hardware, during manufacturing or delivery of components.

These vectors are refined into several tactics, techniques and procedures (TTPs) and are implemented in attack scenarios which are usually carried out in four major phases: Preparation – Engagement – Maneuver – Attack [5].

It should be emphasized that the Insider is at the intersection of all threat vectors, making him a key risk factor. Table 1 sets out various categories of Adversary depending on its origin and the nature of its action.

3 ASSESSMENT OF CYBER-ATTACKS ON AN AUGT

We have undertaken a comprehensive and detailed risk analysis of plausible attacks against a generic automated urban guided transport covering the three dimensions – human, cyber, physical – and integrating any kind of adversary and all potential modes of action.

We do not describe in detail this assessment but we rely upon its rigorous reasoning in order to elicit the conditions under which an Insider provides a key advantage to compromise an AUGT through a cyber-attack.

Table 1: Insiders vs. Outsiders [6]–[7].

	Lone Insider	**Group of Insiders**	**Outsider/Insider**	**Outsider**
Attitude	True Insider (lone wolf)	Insider's conspiracy	Outsider sought by Insider Insider controlled by Outsider	Outsider infiltrated in targeted organization
Behavior	Human error (non malicious)	Insider induced by a conspirator	Insider deceived by an Outsider	Outsider masquerading as an employee

3.1 Description of a generic AUGT

The AUGT is a distributed system capable enforcing three main functions [8]:

- automatic train protection (ATP), which determines train location, movement authority (based on train location), route status and enforces ATP profile;
- automatic train operation (ATO), which enables the absence of the driver on board the train, ensuring the fully automatic management of the train in combination with ATP;
- automatic train supervision (ATS), which ATS offers services related to the supervision and management of the train track, such adjustment of schedules, determination of speed restrictions within certain areas and train routing.

The generic AUGT design follows the architectural principles outlined in [9].
The generic AUGT design exhibit important characteristics:

- algorithmic complexity of train control functions that are based on a set of distributed nodes communicating via synchronized messages;
- defense in depth via layering of independent barriers. In particular the transport network is separated from the corporate networks and the internet. Only a few specific interfaces protected by stringent access control remain to allow a set of specific administration services managed by authorized entities;
- the attack surface of technical components is extremely reduced due to safety protections;
- the architecture mixes COTS with proprietary components;
- it enforces a safety model requiring that the train stop in any abnormal situation;

The preliminary analysis showed us that there are three dreaded events (DE) with potential catastrophic consequences: railway accident (DE-1) – systemic disruption of AUGT (DE-2) – stealthy takeover of the system at the cyber-layer (DE-3) (which could entail the two first ones).

There are a lot of attack avenues as shown in Fig. 3.

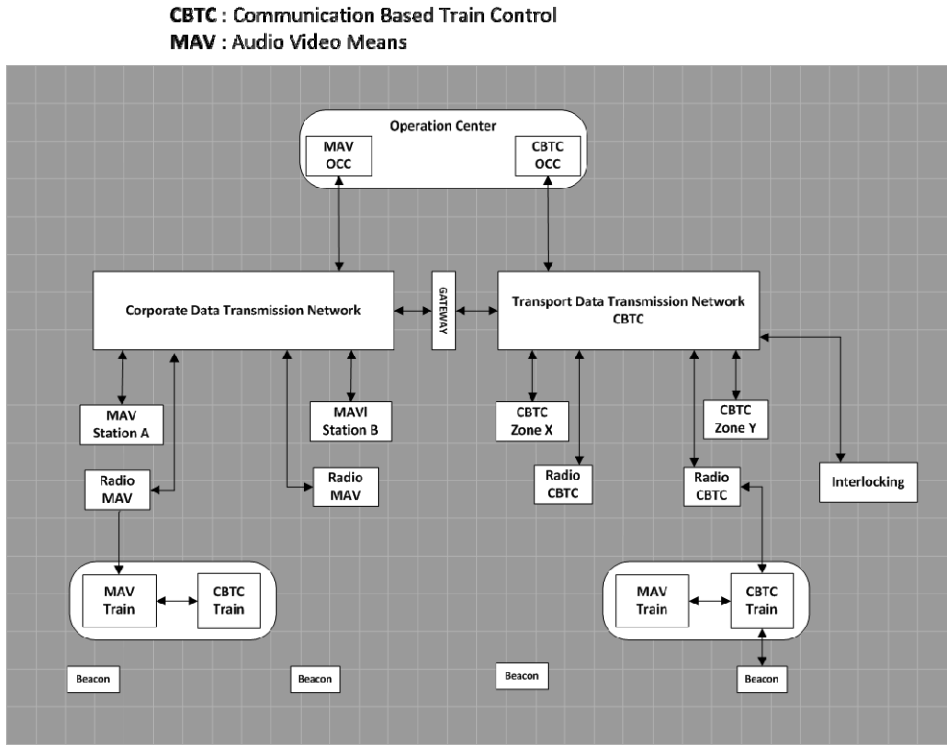

Figure 2: Generic AUGT architecture.

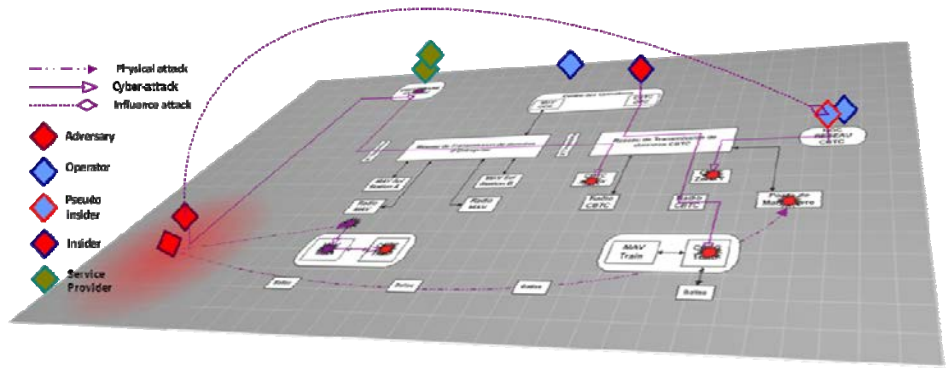

Figure 3: Examples of attack avenues against an AUGT.

The diversity of modes of action for an intended effect raises the issue of choosing between a cyber TTP and a kinetic one. If DE-2 and DE-3 require a cyber-attack against the command and control layer of our system, a physical sabotage remains the simplest way to provoke a railway accident. The whole point of the cyber TTP is in the uncertainty

surrounding the cause of the accident it may create because this uncertainty could affect the transport operator's trust in his own system.

3.2 Analysis of threat actors and vectors

Supply-chain and *Outsourced service* vectors are out of our scope because they depend on an external organization while the risk analysis found that the *Remote access without user assistance* vector cannot overcome the defense in depth.

This assessment has also identified from the AUGT features a set of critical knowledge and access requirements for the Adversary to be able to successfully defeat the system's safety barriers and cause a dreaded event:

- knowledge of specification of at least one safety-critical function to determine an effective mode of action;
- knowledge of architectural layout and identification of critical nodes for recognizing high value targets and identifying potential entry points and attack avenues;
- knowledge of detailed internal design of these nodes and of the communication protocols, to find exploitable vulnerabilities and develop the cyber-weapon;
- access to critical cyber services or physical components in order to deliver and command the cyber-weapon.

Given the purpose of our study, we do not present a detailed profile of all motivated and capable threat actors who could carry out a cyber-attack against an AUGT, we just broke up the set of adversaries into two groups – the true (i.e. self-motivated Insiders and the Pseudo-insiders (i.e. employee(s) under some kind of control by an Outsider).

3.3 True insiders

Firstly, we do not deal with conspiracies of Insiders because the case studies found that they usually aim to steal valuable items [6]. Secondly, the above system's safety features reduce the set of dangerous true Insiders to system's operators and administrators alone. In addition, achieving DE-2 or DE-3 requires the delivery of a very sophisticated cyber-weapon that is beyond the reach of a true Insider. The remaining scenarios are:

- the transmission by an operator of an inappropriate instruction in a particular situation which would lead to an accident;
- the modification of a critical parameter by an administrator.

In both cases, the perpetrator has to take a substantial risk given the rules governing the access to the system's core components and the logging of all privileged actions. Indeed, only people with strong idiosyncratic motivation or psychiatric disorders would attempt such an attack. This issue will not be further dealt with in our paper.

3.4 Collusion between outsider and insider

Whatever the dreaded event, the Adversary must have specific knowledge of and access to the system and the resources and skills needed for developing a cyber-weapon able to bypass or to tamper with the safety barriers.

We can then analyze each phase of the attack lifecycle to determine the significant role an Insider could play and its relationship with an external sponsor.

Note: *TN* is the Transport Network and ***CN*** the Corporate Network.

3.4.1 Phase 1: preparation

This phase consists mainly of operational planning and cyber-weapons development. An in-depth knowledge of safety functions, architectural layout, and technical vulnerabilities is necessary to plan the attack and design the cyber-weapons**.**

Table 2: Requirements for Phase 1 – preparation.

<table>
<tr><th></th><th>[A]- Safety Specification</th><th>[B] - Architectural Layout</th><th>[C] - Technical Vulnerabilities</th></tr>
<tr><td rowspan="2">OSINT</td><td rowspan="2">[OA.1]: Identify key personnel with access to design documentation (→ [HX]).</td><td>[OB.1]: Identify key personnel with access to design documentation (→ [HX]).
[OB.2]: Identify key personnel with cyber access to TN, (→ [HX] → [CB.1]).
[OB.3]: Identify key personnel with physical access to TN, (→ [HX] → [CB.1]).</td><td>[OC.1]: Identify key personnel with access to software programs (source or object), (→ [HX]).
[OC.2]: Identify key personnel with cyber access to TN, (→ [HX] → [CC.1]).
[OC.3]: Identify key personnel with physical access to TN (→ [HX] → [CC.1]).</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="3">CYBINT</td><td colspan="3">[CN]: stealthy entry in CN to steal human resources files and identify key personnel (→ [HX])</td></tr>
<tr><td>[CA.1]: stealthy entry in CN then theft of specification documentation
[CA.2]: stealthy entry in TN then spying to infer functions</td><td>[CB.1]: stealthy entry in TN then eavesdropping of communications to infer the architectural layout</td><td>[CC.1]: stealthy entry in TN then eavesdropping of communications and extraction of safety-related software programs</td></tr>
<tr><td colspan="3">All attack but [CA.1] require a close access to TN that may be executed by an insider</td></tr>
<tr><td>TECHINT</td><td colspan="2">Not Applicable</td><td>[TC]: reverse engineer the software programs and protocol transactions to identify exploitable vulnerabilities
Activity performed inside the Adversary’s facilities</td></tr>
<tr><td rowspan="4">HUMINT</td><td rowspan="2">[HA]: Identify key personnel with access to specifications</td><td>[HB]: Identify key personnel with access to architectural documentation</td><td>[HC]: Identify key personnel with access to software programs archives</td></tr>
<tr><td colspan="2">[HN.1]: Identify key personnel with cyber access to TN
[HN.2]: Identify key personnel with physical access to TN</td></tr>
<tr><td colspan="3">[HX]: Influence key personnel to perform a specific action (theft of documents, implantation of rogue device or software, facilitation of a physical entry etc.)</td></tr>
<tr><td colspan="3">[HS]: Subversion of the Operator by infiltrating an outsider within it’s organization. This condition enables all subsequent phases of the attack</td></tr>
<tr><td>Legend</td><td>OSINT: Open Source Intelligence
CYBINT: Cyber Intelligence</td><td>TECHINT: Technical Intelligence
HUMINT: Human Intelligence</td><td>→ : enables</td></tr>
</table>

The cyber-weapon development is done inside the Outsider's facilities and does not rely on the other phases of the attack.

3.4.2 Phase 2: engagement

The cyber-weapon has to be implanted inside the transport network via a *Close access* or a *User-assisted Remote access*. There are several possible scenarios.

The **Phases 3** (**Maneuver**) and **4** (**Attack**) could be entirely automated or executed by an operator who is either an Outsider physically present in the transport network or an Insider acting on behalf of the Outsider.

For each phase of the attack lifecycle, we have identified the actions that can be performed or facilitated by an Insider. The number and diversity of circumstances clearly show the tactical advantages given to an external Adversary by the involvement of an Insider, which can take two distinct forms:

- an unwittingly assistance to carry out a punctual action;
- an active and deliberate participation under a collusive scheme.

The second case is the most worrying because it allows the Adversary to fully take advantage of the Insider knowledge and privileges.

To go further in the study of the relationship between an Insider and an Outsider, one must understand the process of social influence.

Table 3: Requirements for Phase 2 – engagement.

	[E]: Entry in Corporate Network	**[W]: Implantation of the weapon**
OUTSIDER	**[EO.1]**: physical penetration (Entry by Force) of ***TN*** by an Outsider. **[EO.2]**: physical infiltration (Entry by Ruse) of ***TN*** by an Outsider who deceives the security barriers thanks to the intelligence obtained during Preparation. (This attack may exploit the gullibility of an employee) **[EO.3]**: physical infiltration (Entry by Ruse) of ***TN*** by an Outsider, with the help of an Insider controlled by the Adversary	**[WO.1]**: direct physical insertion in ***TN***
	[EO.4]: entry in ***CN*** by an Outsider who takes over a remote maintenance device. This scenario has several modalities according to the nature of entry (force, ruse, intervention of an insider)	**[WO.2]**: cyber delivery of the weapon in ***TN*** via administration service
INSIDER	**[EI.1]**: physical penetration (Entry by Force) of ***TN*** by an Insider controlled by the Adversary **[EI.2]**: physical infiltration (Entry by Ruse) of ***TN*** by an Insider controlled by the Adversary **[EI.3]**: physical entry of ***TN*** by an Insider, abusing his privileges, controlled by the Adversary	**[WI.1]**: direct physical insertion in ***TN*** **[WI.1]**: user-assisted physical insertion (e.g. via a deceptive like an USB key device) in ***TN***t
	[EO.4]: takeover of a remote maintenance device in ***CN*** by an Insider controlled by the Adversary **[EO.4]**: direct exploitation of a remote maintenance device by a privileged Insider controlled by the Adversary	**[WI.3]**: cyber delivery of the weapon in ***TN*** via administration service

4 INFLUENCE METHODS AND TECHNIQUES

Based on a review of the several works by academic as well as intelligence and military communities we build a general model describing the wide array of influence methods, from co-optation to subversion, through deception and coercion [10]–[15].

The tactics [4]–[7], [10]–[12], can provide the adversary with a means to control an insider targeted to an extent variable (according to the tactic used and the target's predispositions). The tactics [2], [6], [7] are used in the unintentional assistance scenarios. The infamous social engineering falls within this class.

We put aside [3] and [9] because they aim at the absence of action, and [8], which does not apply to a single user.

There is no global framework integrating in a consistent manner all manipulation tactics and techniques. That is why we separate the analysis of persuasion from deception from that of deception, we chose the works by Cialdini [12], Waltz et al. [15] and Burkett [16] because they are relatively complementary.

The remainder of the paper will focus on manipulation subclasses, persuasion and deception, because they are by far the most interesting tactics.

Table 4: Influence tactics.

	Target	Tactic	Definition
INDUCEMENT	Behavior	**[1] – Argumentation**	Develop logical arguments to convince an actor
		[2] – Suggestion	Seduce or put an idea into the mind of an actor
		[3] – Dissuasion	Discourage an actor to acting in a certain way
	Attitude	**[4] – Co–optation**	Bring an actor inside a social or a political system
		[5] – Bribery	Give money to an actor to acting in a certain way
MANIPULATION	Behavior & Attitude	**[6] – Deception**	Mislead an actor by fabrication, distortion, or falsification of evidence to induce him to react in a certain manner
		[7] – Persuasion	Convince an actor to freely change his own attitude or behaviors regarding an issue
		[8] – Disinformation	Transmit false, incomplete or misleading information to a group of actors
COERCION	Behavior	**[9] – Deterrence**	Avert an actor from acting in a certain way by threatening him
		[10] – Compellence	Make an actor take actions by threatening him
	Attitude	**[11] – Indoctrination**	Make an actor adopt certain beliefs by suppressing all possibility to consider alternative ideas
		[12] – Subversion	Alter definitively the free will of an actor by a combination of physical pressures and mind-control techniques

4.1 Model of persuasion

From an abstract point of view, persuasion is based upon "the cognitive response law of influence" which states that a successful persuasion tactic directs and channels thoughts in order to disrupts negative thoughts while promoting positive thoughts about the proposed course of action.

Cialdini, one of the most influential researcher on this topic, has enumerated six main principles underlying persuasion:

- reciprocity: all humans feel an obligation to try to repay in kind what another person has provided;
- commitment and consistency: the desire for consistency is a central motivator of our behavior. Society generally seems to spurn members who are inconsistent;
- social proof: Once individuals have invested deeply and sacrificed much, they will go to great lengths to hold on to the beliefs to which they had become committed;
- liking: we like people who are like us;
- authority: authority always induces obedience;
- scarcity: when an item is less available humans tend to believe it is more attractive. On a deeper level, when an item or option is offered and then withdrawn, humans tend to desire that item or option even more.

4.2 Model of deception

Deception is simply a combination of manipulation, distortion, falsification, suppression or fabrication of evidence to induce a target to have a reaction advantageous to the deceiver's interests. The goal of deception is generally to make the target more vulnerable to subsequent actions. Deception is fundamentally a tactic aiming at manipulating perceptions and is always a combination of four complementary methods:

- providing the target with real data and accurate information;
- hindering the target from accessing real data or accurate information;
- providing the target with false data and wrong or misleading information;
- determining the focus of target's attention then manipulating what the target registers.

By manipulating the way the target registers, processes, perceives, understands data and/or information, deception influences its beliefs and behaviors.

5 DEFENSE STRATEGY

A classical cybersecurity strategy deals mostly with technical weaknesses, which could be sought by intensive tests or thorough investigations like code analysis, and their particular exposure (i.e. attack surface). For human beings, there is no such testing procedures, we merely determine the general classes of predispositions of malevolent behavior.

Numerous studies – ranging from formal academic efforts to in-depth case reports – have revealed a common set of factors that, taken together, seem to form a critical pathway whose analysis help us identifying the interrelationships between an Insider's activities and its most crucial points [17]–[18].

These fundamental factors are:

- personal predispositions such as motivation (e.g. identification with a cause or financial incentive), perceived legitimacy of a malicious behavior, acceptability of costs and risks;

- personal, financial or professional stressors;
- emotional fallouts that leave people vulnerable to persuasion;
- organizational, cultural and cognitive biases that make people vulnerable to deception;
- the failure or absence of procedural responses to prevent or detect a malicious behavior;
- the absence of a comprehensive approach incorporating both human and technical factors etc. resulting in an inadequate management of the Insider's problem.

In a later stage, this work will serve as a basis for defining an effective defense strategy.

CONCLUSION

From a rigorous study of potential cyber-attacks against an Automated Urban Guided Transport, we have identified and examined the circumstances where an Insider could play a decisive part, notably in partnership with an external Adversary.

In a second phase, we analyzed the principles of influence that enable such collusions.

REFERENCE

[1] US, Department of Defense, Cyberspace Operations, JP, pp. 3–12, 15–17, 2013.
[2] Caire, J. et al., Expression des Besoins et Identification des Objectifs de Résilience. *Resilience des systèmes numériques*, 22e édition des journées C&ESAR, 2015.
[3] US Cyber Command, Assessing Actions along the Spectrum of Cyberspace Operations, 2013.
[4] US Cyber Command, Operation Gladiator Shield, pp. 3–4, 2011.
[5] US Office of the Director of National Intelligence, Cyber Threat Framework, 2017.
[6] Hoffman, B. et al., *Insider Crime*, Rand Report, **3782**, pp. 22–23, 1990.
[7] US Department of Homeland Security, Risk to US Critical Infrastructure from Insider Threat, 2013.
[8] IEC, Railway applications Urban guided transport management and command/control Systems: Part 1: System principles and fundamental concepts, IEC 62290-1, 2007.
[9] IEEE, Standard for Communications-Based Train Control (CBTC) Performance and Functional Requirements, IEEE 1474.1, 2004.
[10] Davis, P.K., Deterrence by Denial, Rand Report WR 1027, 2014.
[11] Francart, L., La guerre du sens, Edited by Economica, 2000.
[12] Cialdini, R., *Influence: The Psychology of Persuasion*, Harper Business (ed.), 2006.
[13] Perloff, R., *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*, Edited by Routledge, 2013.
[14] Pratkanis, A.R. et al., *Science of Social Influence*, Edited by Psychology Press, 2007.
[15] Waltz, E. et al., *Counter-deception for National Security*, Edited by Wiley, 2007.
[16] Burkett, R., An Alternative Framework for Agent Recruitment: From MICE to RASCLS. *Studies in Intelligence,* **57**(1), 2013.
[17] Shaw, E. et al., The psychology of dangerous insider. *Security Awareness Bulletin*, pp. 2–98, 1998.
[18] Shaw, E., Application of the critical-path method to evaluate insider risks. *Studies in Intelligence*, **59**(2), 2015.