RASCLS VS. RANSOMWARE: A COUNTERINTELLIGENCE FRAMEWORK FOR CYBERSECURITY EDUCATION

BRYSON PAYNE, University of North Georgia
Bryson.Payne@ung.edu

EDWARD MIENIE, University of North Georgia
Edward.Mienie@ung.edu

ABSTRACT

This article advocates using the RASCLS v Ransomware (RvR) framework to detect, defend against, and defeat cyber-attacks. RvR employs conventional counterintelligence practices such as the traditional MICE+ G and more modern RASCLS counterintelligence framework to detect, defend against, and defeat cyber-attacks. The MICE+ G framework holds that people betray their organizations and countries because of money (financial problems or goals), ideology (beliefs), coercion/compromise, ego/extortion, and grievances. RASCLS offers similar rationales: reciprocation, authority, scarcity, commitment/consistency, liking (befriending), and social proof.

Keywords: *counterintelligence, cybersecurity, MICE+ G, phishing, ransomware, RASCLS, social engineering*

INTRODUCTION

The past decade has seen an exponential increase in destructive malware attacks, identity theft, corporate and government espionage, intellectual property theft, and nation-state-sponsored ransomware attacks. Social engineering, using deception to manipulate individuals into divulging confidential information, is a common factor in spreading these malicious attacks. Phishing emails are the most prevalent form of social engineering online: over 90% of computer-based attacks and breaches employ phishing tactics (Verizon, 2017), 74% of corporate cyber-espionage actions involve phishing (Jentzen, 2018), and 70% of breaches associated with nation-state or affiliated actors involve phishing (Jentzen, 2018). Numerous high-profile ransomware attacks occurred during the past several years against companies, individuals, hospitals, municipalities, and military and government agencies (Payne & Mienie, 2021). Newer double-extortion ransomware variants compound the damage. These new forms of ransomware steal a copy of an organization's files before encrypting them, demand a ransom for decryption, and a second ransom for not posting the stolen data on the dark web.

Social engineering leverages human weaknesses by manipulating people into providing private and sensitive information. Businesses spend over $300 billion annually on cybersecurity globally, up from as little as $3.5 billion in 2004 (Braue, 2021). Notwithstanding these expenditures, malicious cyber actors continue to attack and infiltrate millions of personal and

organizational systems through emails, including the most sensitive networks housed by the private and public sectors. These attacks and infiltrations include the highest levels of government, military, and intelligence organizations.

Prior research has examined behavioral responses to anti-phishing education (Downs et al., 2007; Huang et al., 2009), but few training techniques seem to move the needle toward better behavioral outcomes. An estimated 90% of computer-based attacks emanate from ubiquitous emails. The billions of dollars spent on computer and network training for millions of employees and private users have not yielded the desired result, safe and secure Internet communications. However, through counterintelligence (CI) education, we can train computer and network operators, especially government, military, and intelligence officials, to detect, defend against, and defeat cyber-attacks.

THE MICE+G AND RASCLS FRAMEWORKS

In traditional counterintelligence doctrine, treason and treachery are attributed to *money, ideology, coercion or compromise, ego,* and *grievance* (MICE+G). More recently, the *reciprocity*, *authority*, *scarcity*, *consistency*, *like,* and *social proofs* (RASCLS) framework has been used to identify potential enemies, traitors, and cyber criminals. This article argues that the MICE+G and RASCLS frameworks can help educate and train members of the public and private sectors to detect, defend against, and defeat cyber-attacks.

RASCALS v Ransomware Training (RvR) includes an examination of five infamous cases of treason and betrayal using the MICE+G and RASCLS counterintelligence frameworks. The cases are the U.S. Navy Chief Warrant Officer John A. Walker's 1967 Russian spy affair; the Cambridge Five scandal (1934-1970); the activities of East German Stasi activities (1950-1990); FBI agent Robert Hanssen betrayal (1979-2001); and Russian Colonel Oleg Penkovsky spying activities against Russia (1960-1963).

MICE+G

Hugh and Wilson's (2017) *The Secret State: A History of Intelligence and Espionage* portrayal of five infamous cases of treason and betrayal provides prescient examples of the MICE+G framework.

- Money (M): Chief Warrant Officer Walker's financial difficulties contributed to his decision to spy for Russia.
- Ideology: The Cambridge Five's communist leanings influenced their decision to spy for the Russians.
- Compromise (C): The Stasi and its spy chief Markus Wolf notoriously snared U.S. and allied officials in sexually compromising situations.
- Ego (E): FBI Special Agent Robert Hanson's notorious ego led to his disdain for his organization and subsequent sharing of U.S. intelligence documents with Russian officials.

- Grievance (G): Russian Colonel Oleg Penkovsky felt he had been unfairly denied a much-deserved promotion. His grievance contributed to his decision to spy for the U.S. and the U.K.

RASCLS

Cialdini's (1984). *Influence: The Psychology of Persuasion's* RASCLS framework offers a comparable method to the MICE+G framework. Burkett's (2013) An Alternative Framework for Agent Recruitment breaks RASCLS down for us.

- "R" is for reciprocity. Potential recruited targets may develop a sense of obligation to handlers (case officers) that provide means to deal with problems or goals.
- "A" represents authority. Case officers may project an image that they are members of a powerful organization or government. Case officers must be obeyed.
- "S" is for scarcity. Case officers may promote the idea that information that is not readily available is more valuable in the present, and its value will diminish with time. Time is of the essence; if the recruited target hesitates, the information and the target will be less valuable.
- "C" represents commitment and consistency. Recruited targets must demonstrate commitment and consistency. They must be faithful to the cause and consistently contribute to its success.
- "L" represents "liking." People like being liked and having friends. Case agents befriend their recruits, albeit falsely.
- "S" is for social proof. Case officers must demonstrate to potential targets that others have similarly betrayed their organizations and nations and that doing so is the "right thing" to do.

MICE+G AND RASCLS APPLIED TO CYBERSECURITY

The same psychological methods that intelligence officers use to recruit spies apply to social engineering in the cyber realm. Social engineering employs deception to manipulate individuals into giving up confidential information or performing other acts against their own best interest or the interests of their organization or nation. This research utilizes CI training based on the MICE+G and RASCLS frameworks to combat cyberattacks.

The most fundamental CI concept to empower people against social engineering and related cyberattacks is "everyone is a target." All computer and Internet users must be security conscious. Military and government agents are trained in CI techniques before traveling abroad to alert them to the dangers of being manipulated by overseas adversaries. One of the first steps to this CI training is to make the subject aware that they are a target for foreign intelligence operatives. Similarly, the RvR training framework trains users to recognize potential malicious actors.

Cybercriminals, terrorist organizations, and adversarial nation-state actors are constantly searching for vulnerable individuals who might be duped into surrendering their personally identifiable information (PII) and sensitive/classified information. A CI approach to cybersecurity begins with a heightened awareness of the presence of malicious actors. In the RvR training framework, trainees are exposed to the MICE+G and RASCLS frameworks. Next, trainees apply the tenets of the frameworks to fictitious scenarios that include social engineering, phishing, and other cyber-attack tactics.

CONCLUSION

The MICE+G and RASCLS frameworks adapted to CI can prepare people from all walks of life to deter, detect, and defeat potential malicious social engineering and other nefarious cyber activity.

RECOMMENDATIONS

Policymakers, organizations, and educators should consider adopting concrete, behavioral approaches to cybersecurity CI awareness training, such as the RvR framework, to prepare their workforces and students to detect, defend against, and defeat all cyber threats.

REFERENCES

Braue, D. (2021). Global cybersecurity spending to exceed $1.75 trillion from 2021–2025, *Cybercrime Magazine*. https://cybersecurityventures.com/cybersecurity-spending-2021-2025/

Burkett, R. (2013). An alternative framework for agent recruitment: From MICE to RASCLS. *Studies in Intelligence 57*(1).

Cialdini, R. (1984). *Influence: The psychology of persuasion.* Quill/William Morrow, 1984.

Downs, J. S., Holbrook, M., & Cranor, L. F. (2007). Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. ACM.

Huang, H., Tan, J., & Liu, L. (2009, June). Countermeasure techniques for deceptive phishing attacks. In *2009 International Conference on New Trends in Information and Service Science*.

Hughes-Wilson, J. (2016). *The secret state: A history of intelligence and espionage*. Pegasus Books, Ltd.

Jentzen, A. (2018). Phishing, pretexting, and data breaches: Verizon's 2018 DBIR.

Payne, B.R. & Mienie, E.L. (2021). Multiple-extortion ransomware: The case for active cyber threat intelligence. *Proceedings of the 20th European Conference on Cyber Warfare and Security (ECCWS)*, 331–336, Chester, UK.

Verizon. (2017). 2017 Data breach investigations report. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.verizon.com/business/verizonpartnersolutions/business/resources/reports/2017_dbir.pdf