2020 IMEKO TC-19 International Workshop on
Metrology for the Sea
Naples, Italy, October 5-7, 2020

Triggering Cyber-electronic Attacks in Naval Radar Systems

Walmor Cristino Leite Junior[1,2], Alan Oliveira de Sá[1,2]

[1] *Brazilian Naval War College, Simulation and Scenarios Laboratory/Postgraduate Program in Maritime Studies, Rio de Janeiro, Brazil, walmor.clj@outlook.com*
[2] *Admiral Wandenkolk Instruction Center, Rio de Janeiro, Brazil, alan.oliveira.sa@gmail.com*

***Abstract* – The present paper discusses relevant aspects related to hybrid attacks involving cyber warfare and electronic warfare in naval radar systems. It addresses how such attacks can be implemented, showing that Electronic Attacks (EA) can be used to remotely trigger a cyber threat hosted in a radar computational system. The concept is demonstrated through simulations where a template matching technique is used to acknowledge the EA and, thus, trigger the cyber threat. The results show the effectiveness of the technique as a tool for activating malicious code previously installed in a radar system.**

I. INTRODUCTION

Cyber Warfare (CW), which seeks to explore and manipulate digital information, is becoming increasingly relevant in the international context. Advanced cyber attacks have been documented and the studies generated for their understanding shows the feasibility of development of others even more powerful and with great potential to achieve strategic objectives [1,2,3]. Among these attacks are the malwares, *i.e.* malicious codes that aim to interfere with the functioning of systems. Stuxnet [4], an example of malware supposedly produced by Nation-States, was able to delay a country's nuclear program by a few years [5]. In the military operation *Orchard*, according to the literature [6,7,8], the Israeli air force attacked a Syrian facility without being noticed thanks to a malicious cyber mechanism installed in the Syrian radar system. One hypothesis raised in the literature [6,7,8] regards to the possibility that an Electronic Attack (EA) – *i.e.* an attack performed in the electromagnetic spectrum – was used to unleash a cyber attack capable of hindering the radar computational process. Such integration of electronic and cyber attacks presents itself as a new trend in modern warfare, where the resulting *cyber-electronic* attacks represent a novel class of threats to be addressed [9].

In the maritime sector, radar systems are used as relevant sensors for navigation safety or as a source of information for integrated navigation systems. Note that a compromised radar system may result in serious risks to the vessels' safety, with possible impacts in a wide range of areas (*e.g.* economic, environmental, defense, etc.). For this reason, it is important to study how such kind of cyber-electronic attacks can be implemented and seek for possible countermeasures.

This paper presents how a template matching technique can be used in a cyber-electronic offensive [9] to detect specific EA patterns and, thus, use this information to trigger a malicious cyber process in a radar system. The main contribution of this paper is to demonstrate, for the sake of awareness, a mechanism that can be used as a link between an EA and a cyber weapon. More specifically, the mechanism is used to allow an EA to trigger a cyber weapon previously installed in the naval radar system. The effectiveness of the proposed mechanism is assessed through simulations in Python, where the target is a generic radar system used for maritime navigation.

The rest of this work is organized as follows: Section II presents the related works. Section III describes the mechanism proposed in in this work to allow the communication between the EA and the cyberattack in a radar system. Section IV presents the simulation results. Finally, Section V brings the conclusions.

II. RELATED WORKS

The disclosure of the Stuxnet malware in 2010 showed the details of a worm endowed with a surprising level of complexity [4,5]. Its refinement raised concerns about the development of specialized, high skilled and complex cyber weapons, with multidisciplinary design. The literature [4,5] shows that it would not be possible to develop such a sophisticated weapon without extensive technical support of highly qualified human resources from different technical fields (*e.g.* Information and Communication Technology, Control Engineering and Nuclear Engineering). It would have been created by State institutions to achieve strategic objectives in the international environment [5]. The target of Stuxnet was an Iranian nuclear enrichment plant that had its operation impaired, delaying the country's nuclear program by some years. Today, several studies on it are available, showing that such attack model can be used as inspiration for individuals with malicious intentions against other critical targets. The same concept of multidisciplinary attack can be used to impair other platforms, including

systems and sensors used in naval environments, which may have cyber vulnerabilities – intentionally implanted or not.

In [9], the authors discuss the concepts of hybrid attacks in the scope of sea power, where the cyber, electronic and kinetic warfare can be integrated to accomplish specific tactical and strategic purposes. The separate application of these kinds of warfare has been usual in modern military operations, however it is noticed that there is a trend for these warfare dimensions to merge so that actions in one of them cause effects in the others. An example of hybrid attack is sown in [10], where the authors demonstrate an EA (more specifically a GPS spoofing attack) that is able to produce a kinetic effect on a ship navigation.

Among the possible kinds of hybrid attacks discussed in [9], this paper focuses on the cyber-electronic attack. More specifically, it addresses a particular attack against naval radar systems which, to the best of our knowledge, is not explored in the literature. According to [9], a cyber-electronic attack is an offensive where Electronic Warfare (EW) actions seek not only to manipulate the tactical information obtained through the electromagnetic spectrum (as in the traditional EW), but also to manipulate the computational process of the target system.

In [11], the authors present an EA technique able to forge multiple false targets, with different ranges, within the radar detection range. The purpose of their technique is to produce multiple fabricated targets and, thus, make the radar operator unable to distinguish between the real target and the false targets. Note that in their case, the target detection information is manipulated, but the radar computational process continues to run normally. To make such EA able to manipulate the computational process, it would be necessary to have in the radar system a mechanism prepared to acknowledge the false information produced by the EA as a command to trigger the malicious cyber mechanism responsible for manipulating the system behavior.

Note that for such a cyber-electronic attack, it is necessary to have a cyber component previously implanted in the radar computing system. On this aspect, the literature report vulnerabilities implanted in air gapped systems (which is often the case of naval radar systems). These vulnerabilities can be implemented either in software, as in the Stuxnet [12], or in hardware through supply chain attacks, as in [6,13]. Special attention should be given to the operation *Orchard*. According to [6], commercial off-the-shelf microprocessors contained in the Syrian radar might have been purposely fabricated with a hidden hardware backdoor (referred to as *kill switch*) which, by receiving a preprogrammed code had its functions disrupted and temporarily blocked the radar.

In this context, the aim of this work is to show – for awareness purpose – how the electronic and cyber warfare can be linked. As previously discussed, in [11] the authors present an EA able to produce multiple forged echoes for radar systems. In [6], the author presents clues about the implantation of a cyber vulnerability to affect radar systems, but does not explain how such vulnerability can be triggered as the convenience of the attacker, especially if radar computers are air gapped and the only path to send commands to a previously installed vulnerability is through the radar antenna. In this work we demonstrate a mechanism that can be used to link the electronic and cyber warfare domains – a key element for the construction of a cyber-electronic attack.

III. MECHANISM FOR CYBER-ELECTRONIC ATTACK

In the cyber-electronic attack addressed in this work, it is assumed that the electromagnetic spectrum is used by the attacker to send a sequence of forged pulses to the radar receiver, as in [11], which is coded in time/range to represent a command to the cyber mechanism hosted in the radar. Once the command is acknowledged, the cyber component of the attack can start to manipulate the radar computational process to perform malicious actions, such as reset the system, stop to update the Plan Position Indicator (PPI), or even record and replay scenarios. The focus of this work is not on the generation of the forged radar echoes (an action in the EW domain represented in Figure 1), neither in the details about the manipulation of the radar computational process (an action in the CW domain represented in Figure 1). The focus of this work is on the linking mechanism that lies between both domains to make a cyber-electronic attack feasible in a naval radar system. The mechanism herein proposed for this task is based on a template matching technique [14].

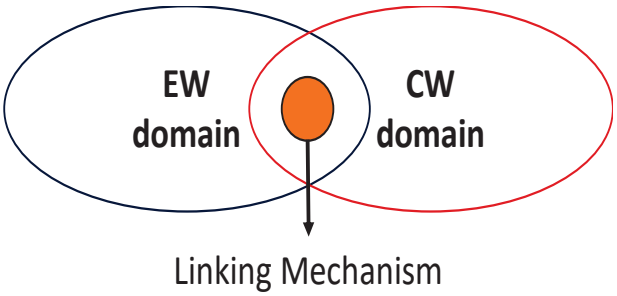

Fig. 1. Linking mechanism between EW and CW domains

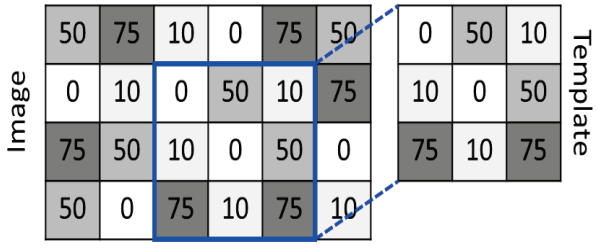

Fig. 2. Example of a template matching

The template matching technique is used in image processing to find small parts of an image that correspond to a model (template) image. To do so, it is defined a template to be searched in a main image. The main image in analysis and the template are divided in pixels, as shown in Figure 2. Then the template is moved over the main image, in a search process throughout all the main image's area. For each position assumed by the template in this scanning process over the main image, a similarity index is computed. The similarity index quantifies the similitude between the template and the piece of the main image being compared. If the index is higher than a previously defined threshold, then the template image is considered to be detected in the main image. This exhaustive search operation demands a considerable computational cost, proportional to the sizes of the images. On the other hand, it provides a high degree of effectiveness in searching for patterns in images [14].

Note that the degree of similarity between the template and a piece of the main image is established by comparing intensity values of each of their pixels. Among the available methods to compute the similarity coefficient, there are: the Sum of Absolute Differences (SAD), the Sum of Squared Differences (SSD), and normalized cross correlation. In this paper, the Pearson cross correlation (PCC) [14] is used (1):

$$corr = \frac{\sum_{i=1}^{N}(p_i + p)(a_i - a)}{\sqrt{\sum_{i=1}^{N}(p_i - p)^2}\sqrt{\sum_{i=1}^{N}(a_i - a)^2}} \qquad (1)$$

wherein, p_i is the intensity of pixel i in the template; p is the average intensity of the pixels of the template; a_i is the intensity of the pixel i in the patch of the image; a is the average intensity of the pixels in the patch of the image; N is the number of pixels. Note that this method presents a normalizing term in the denominator, which gives it invariance to global changes in brightness [14], and the results always lie within a defined range [−1, 1].

IV. RESULTS

The mechanism for cyber-electronic attack described in Section III was evaluated through simulations on a computer with an Intel i7 processor of 2.5 Ghz, 8G RAM DDR3 memory, running Microsoft Windows 10, 64 bits. The radar environment was simulated in the Cinematic Radar Simulator v.2.0 and the template matching mechanism for cyber-electronic attack was implemented and simulated in Python.

It is assumed that the cyber component of the attack (the malware) is already installed in the radar, given that the exploitation mechanisms to install it in the radar computational system is out of the scope of this paper. Also, considering that the implementation of the EA component of the attack is not in the scope of this paper, it is assumed that the remote command (a sequence of false echoes) is generated and transmitted through a Digital Radio Frequency Memory (DRFM) technique [11]. The command is received and processed by the radar, and displayed as an image in the PPI screen, such as any other received echoes (false or not).

In the simulations herein presented, the Python code scans the graphical interface (the PPI) produced by the radar simulator in order to identify the attack commands received from the EA component of the offensive. To evaluate the effectiveness of the proposed mechanism, in this work, the chosen attack command consists of a sequence of five false echoes, which produces a sequence of five points displayed in the direction where the DRFM transmitter is. Once this pattern is detected, it can be used to trigger a malicious action in the naval radar system.

To validate this hypothesis and test the effectiveness of the command detection method, 30 fictitious scenarios were generated using the radar simulation software in order to represent real situations where a naval platform could be. Clutter/target echoes that might affect the command detection were randomly inserted in the PPI. Figure 3 shows an example of scenario used in the simulations. The triggering command is highlighted.

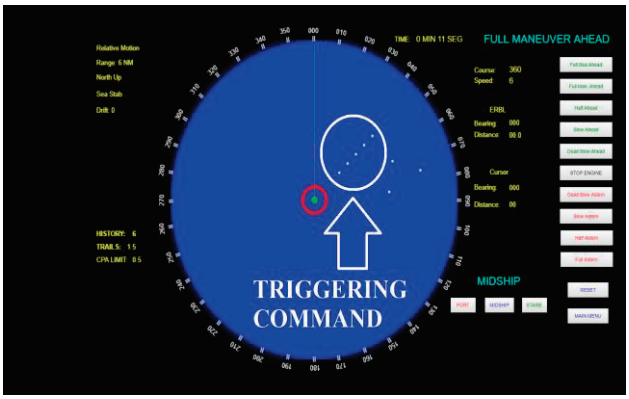

Fig. 3. Example of radar screen used in the simulations

It is worth mentioning that the attacker is transmitting the EA signal that generates triggering command shown in the screen, and that the signal can come from any direction, depending on the DRFM transmitter location. Thus, it is necessary to consider different angles from which the triggering command could be received. For the sake of simplicity, variations of 1 degree are considered, so the attacker could emit from the directions 000, 001, 002, 003 and so on. Considering these possible different Angles Of Arrival (AOA), the template containing the triggering command pattern is also rotated in steps of 1 degree during the search process throughout the PPI. This template matching search is executed throughout all the PPI screen until the algorithm finds a match or until all possibilities along the screen are tested. During the search process, the test image (*i.e.*, the PPI screen) is read and

converted to grayscale. This serves to eliminate possible color variations, performing only the analysis of the pixel intensity. The template is also processed in grayscale for the comparison. To implement the algorithm, the libraries Numpy, cv2 and Pillow were used. The implementation is shown in Figure 4.

```
import numpy as np
import cv2
from PIL import Image

import time

ini = time.time()

for i in range(179):

 print (i)

 colorImage = Image.open('tamplate.png')

 rotated = colorImage.rotate(i)

 rotated.save('tamplate 2.png')

 img_bgr = cv2.imread('Imagem teste 5.png')
 img_gray = cv2.cvtColor(img_bgr, cv2.COLOR_BGR2GRAY)

 template = cv2.imread('tamplate 2.png',0)
 w, h = template.shape[::-1]

 res = cv2.matchTemplate(img_gray,template,cv2.TM_CCOEFF_NORMED)
 threshold = 0.7
 loc = np.where(res >= threshold)

for pt in zip(*loc[::-1]):
     cv2.rectangle(img_bgr, pt, (pt[0]+w, pt[1]+h), (0,255,255), 2)
     cv2.imshow('detected', img_bgr)

fim = time.time()

print ("Tempo de execução: ", fim-ini)
```

Fig. 4 Triggering mechanism implementation in Python

Five threshold levels were assessed: 0.3, 0.4, 0.5, 0.6, 0.7. Recall that the computed PCCs are compared with the threshold levels in order to decide if a match was found or not (see Section III). Each threshold level was assessed using the set of 30 different scenarios. The values corresponding to the confusion matrix for each threshold level are compiled in Table 1. The performance of the triggering mechanism for each threshold level is also depicted in Figure 5.

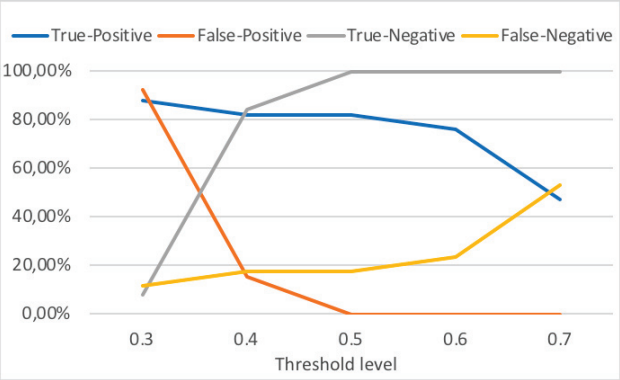

Fig. 5. Performance of the triggering mechanism

The situation of True-Positive (TP) refers to the case where the triggering command is present in the PPI and there is a match with the template. False-Positive (FP) is the case in which the triggering command is not present in the PPI, but there is a match with the template. True-Negative (TN) occurs when the triggering command is not present in the PPI and there is no match with the template. Finally, the False-Negative (FN) occurs when the triggering command is in the PPI but it is not detected. Based on the results, lowering the threshold increases the TP rate, but also increases the FP rate (which may cause fortuitous and unwanted attack activations). On the other hand, increasing the threshold decreases the FP rate, but also decreases the TP rate (which reduces the attack effectiveness). According to the results, the best threshold from the attacker point of view is 0.5. Note that with this threshold the attacker is able to obtain the maximum TP rate (82.35%) without false positives. It means that, with this threshold, considering the evaluated scenarios, the probability of an accidental attack activation tends to 0% (which is important to avoid the attack disclosure) and the attacker has 82.35% of probability in successfully activating the cyber component of the attack in the first attempt. Note that, with two attempts the probability of having the attack properly activated in at least one of the attempts increases to 96.88%.

Table 1. Performance Rates

Threshold	TP	FP	TN	FN
0.3	88.24%	92.31%	7.69%	11,76%
0.4	82.35%	15.38%	84.62%	17,65%
0.5	82.35%	0%	100%	17,65%
0.6	76.47%	0%	100%	23,53%
0.7	47.06%	0%	100%	52,94%

V. CONCLUSIONS

Considering the theoretical framework presented and the simulations carried out, it is possible to realize that EA and cyberattacks can be linked to each other, forming a cyber-electronic attack capable of affecting naval radar systems. The attack exploits the fact that the radar, as a sensor, can be considered an open door for commands. It is possible to use image processing techniques to trigger a malicious code previously installed on a naval radar system with a good accuracy and effectiveness, maintaining the due safety against accidental activations. Even with all the information security devices, all computer systems are subject to the risk of being infected by malware. This mechanism can be used for the benefit of a naval operation, being activated at the most opportune moment for the attacking force. For future work we plan to evaluate the performance of the proposed mechanism in a real system and investigate countermeasures to mitigate this threat – such as tools to verify the integrity of the software used in naval radars.

REFERENCES

[1] S. McLaughlin et al., "The Cybersecurity Landscape in Industrial Control Systems," in Proceedings of the IEEE, vol. 104, no. 5, pp. 1039-1057, May 2016.

[2] G. Liang et al., "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," in IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317-3318, July 2017.

[3] A. O. de Sá, L. F. R da C. Carmo, R. C. S. Machado, "Bio-inspired Active System Identification: a Cyber-physical Intelligence Attack in Networked Control Systems," in Mobile Networks and Applications, pp. 1-14, October 2017.

[4] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, May-June 2011.

[5] K. Zetter, "Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon", Broadway books, 2014.

[6] S. Adee, "The Hunt For The Kill Switch", in IEEE Spectrum, vol. 45, no. 5, pp. 34-39, May 2008.

[7] R. R. Dipert, "Other-than-Internet (OTI) cyberwarfare: challenges for ethics, law, and policy", Journal of Military Ethics, vol. 12, no. 1, pp. 34-53, 2013.

[8] R. A. Clarke, R. K. Knake, "Cyber war", Old Saybrook: Tantor Media, Incorporated, 2014.

[9] A. O. Sá, R. C. S. Machado, N. N. Almeida, "The Convergence of Cyber, Electronic and Kinetic Warfare Within the Scope of Sea Power", Journal of the Brazilian Naval War College, vol. 25, pp. 89-128, 2018.

[10] J. Bhatti, T. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection", Navigation, vol. 64, pp.51-66, 2017.

[11] A. Almslmany, C. Wang and Q. Cao, "Advanced deceptive jamming model based on DRFM Sub-Nyquist sampling," 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST), Islamabad, 2016, pp. 727-730.

[12] N. Falliere, L. O. Murchu, E. Chien, "W32. stuxnet dossier", Symantec, 2010.

[13] J. Robertson, M. Riley, "The big hack: how China used a tiny chip to infiltrate US companies", Bloomberg Businessweek, vol. 4, 2018.

[14] Y. M. Tavares, N. Nedjah, L. M. Mourelle, "Embedded implementation of template matching using correlation and particle swarm optimization", International Journal of Bio-Inspired Computation, 2018 Vol.11 No.2, pp.102 – 109.