Refined Concepts of Massive and Flexible Cyber Attacks with Information Warfare Strategies

Horatiu Moga[1], Mircea Boscoianu[2], Delia A. Ungureanu[3], Florin D. Sandu[4], and Razvan Boboc[4]
[1]National Agency for Fiscal Administration, Braşov, Romania
[2]Air Force Academy, Brasov, Romania
[3]Automation and Information Technology Department, Transilvania University of Brasov, Romania
[4]Electronics and Telecom Department, Transilvania University of Brasov, Romania
Email: horatiu.moga@gmail.com, boscoianu.mircea@yahoo.com, {deliau, sandu, razvan.boboc}@unitbv.ro

***Abstract*—The purpose of this research is to deepen the concepts of massive and respectively flexible cyber-attacks. These two concepts have been connected with three macroeconomic dimensions, cost for national security, public and private cost for nonmilitary and cost for productive investment to indicate the economic state of the actor state, as well as his motivation to choose a mechanism of cyber space attack. Another goal of this research is to define canonical strategies of information warfare which have a great potential for future research in highlighting the elements of social engineering, cyber deception and counter-cyber deception, useful when information is incomplete.**

***Index Terms*—massive cyber attack, flexible cyber attack, kali linux, networks of unmanned systems resource management**

I. Introduction

The purpose of this research is to deepen the concepts of massive and respectively flexible cyber-attacks [1], [2]. These two concepts have been treated in two previous works that have as starting points the concepts of flexible and massive nuclear attacks. This research tries to deepen the two ideas in content and respectively in capabilities of analysis and synthesis for a reality that is present in our lives since 2000, after the spread of the Internet worldwide.

To express the content of one of the two concepts we will be using the concepts of costs in order to define the concepts of cost for national security - x_{CNS}, cost for private and nonmilitary public - x_{CPNP}, cost for productive investment - x_{CPI} [3] and to information warfare strategies, respectively [4]. According to the US Department of Defense, information warfare is defined as "any of actions to deny, exploit, corrupt, or destroy the enemy's information and its functions, protecting us against these actions and exploiting the military information functions itself" [4]; this research stablishes a connection between information war strategies and the three costs defined by Gilpin. Thus we will apply typical models of bimatrix game theory, where strategies are typical information war strategies and utility functions are calculated using Gilpin's costs and hardware resources that characterize a nation's cyber infrastructure. Our research will be included in a research framework of Network of Unmanned Systems (NUMS) for mobile robots that are parts of the armies of two belligerent states consisting of aerial (Unmanned Air Vehicles – U.A.V.), land (Unmanned Ground Vehicles – U.G.V.), and water (Unmanned Underwater Vehicles – U.U.V.) vehicles. We consider that the two countries play Defender or Challenger role – the latter is the first one to attack. The targets consist of three components of the national cyber infrastructure [1], [2]:

- Servers - the most important targets in the system and the brain of the whole national cybernetic system.
- Transport information systems – are composed of transport information elements such as copper cables, fiber optics, radio antennas and switches and routers. They are second priority targets.
- Network clients - are all network devices accessed - by the user from desktop computers, laptops, smart phones, tablets, etc. These targets have third priority.

The means of manifestation of NUMS fleets are performed using the three types of primary cyber-attacks addressed in our previous works [1], [2]:

- Software cyber-attacks - performed at the logical level of national cyber infrastructure.
- Radio-electronic cyber-attacks - carried out by means of radio-electronic warfare jamming at antenna systems of national wireless cyber infrastructure segments.
- Physical cyber-attacks - carried out with rockets or precision bombing with conventional or unconventional munitions on national cyber infrastructure components. *(Example: "The best attack with packets date is either a thermobaric bomb, or a nuclear bomb Launched on the server")* [1], [2].

II. Selective Related Work

This research aims to substantiate more deeply the concepts of *Massive Cyber Attack* and *Flexible Cyber Attack*, implemented using NUMS drone fleets whose resources management is subject to the economic costs of each of the belligerents. The resources involved in the

Manuscript received January 5, 2017; revised June 19, 2017.
doi:10.12720/jcm.12.6.364-370

administration and management of both NUMS fleets involve multiple dimensions in terms of technology, economy and management. Thus, in other works the use of drones is involved in areas of interest such as: maritime and rescue operations [5]-[7], meteorology [8], ecology and pollution monitoring [9], traffic monitoring of various types with UAVs [10] monitoring routes, photometry, border guards [11]-[14] agricultural activities [15]. A wide range of options are used for communication technologies and management algorithms, such as cognitive software radio [16] complex identification algorithms [17] or algorithms with fault tolerance for controlling formation of drone [18] or hybrid propulsion [19]. A special approach is dealing with NUMS complex systems integration in test benches of cyber-physical systems–type with internet of things interface [20].

III. Theoretical Aspects

In international relations theory the concept of overexpansion is defined as the expansion of a state or empire due to its various objectives, but which is unsustainable in terms of its resources. According to US researcher Robert Gilpin there are three macroeconomic parameters that can support the overexpansion process of a state [3]:

- Cost for national security - x_{CNS}
- Cost for private and public nonmilitary - x_{CPNP}
- Cost for productive investment - x_{CPI}.

Related to the three aforementioned parameters Robert Gilpin defined five conditions that support the overexpansion process of a state, which in our case will be performed with NUMS fleets. The five conditions referred as "The Gilpin Test" are [3]:

1. Gross domestic product has tumbled

$$\frac{\Delta x_{GDP}}{\Delta t} \to 0 \tag{1}$$

2. Military expenses grow too much compared to the two other costs

$$\frac{\Delta x_{CNS}}{\Delta t} >> \frac{\Delta x_{GDP}}{\Delta t} \; AND \; \frac{\Delta x_{CNS}}{\Delta t} >> \frac{\Delta x_{CPNP}}{\Delta t} \; AND \; \frac{\Delta x_{CNS}}{\Delta t} >> \frac{\Delta x_{CPNP}}{\Delta t} \; AND \; \frac{\Delta x_{CNS}}{\Delta t} >> \frac{\Delta x_{CPI}}{\Delta t} \tag{2}$$

3. Public and private non-military expenses have a pronounced growth compared to the growth of gross domestic product

$$\frac{\Delta x_{CPNP}}{\Delta t} >> \frac{\Delta x_{GDP}}{\Delta t} \tag{3}$$

4. It is unable to achieve the structural change of the economy type because innovative investment is low compared to the other two costs

$$x_{CPI} < x_{CPNP} \; AND \; x_{CPI} < x_{CNS} \tag{4}$$

5. The high level of corruption.

Reviewing the way of defining the concepts of massive and, respectively, gradual cyber-attack from the previous researches, we will treat the two concepts as manifestations of overexpansion achieved with NUMS, which will be defined as follows:

- Massive Cyber-Attack is performed first time with software and radio-electronic cyber-attacks from the NUMS board of Challenger on the cyber infrastructure of Defender;
- Then the Massive Cyber-Attack continues with physical cyber-attacks from NUMS fleet of the Challenger on cyber infrastructure of Defender;
- "The Gilpin Test" is satisfied;
- Massive Cyber Attack assumes all the investment in aggressive politics, which may lead to state bankruptcy;
- Flexible Cyber Attack is performed in three consecutive distinct steps, which are specific to the three types of forenamed primary cyber-attacks, and are correlated with "The Gilpin Test" unmet;
- Flexible Cyber Attack is adaptive to its environment avoiding state bankruptcy.

In the following we will discuss about the steps required for active servers detection from a national cyber infrastructure of the two belligerent states. The first step is to detect DNS servers of each infrastructure using the script (S5), as well as the IP address domain of each infrastructure using the script (S6) for NUMS fleets of the both states [21], [22].

```
ServiceEnumeration(internetDomanin) {
   cd /usr/bin
   ListOfDNSserversOfInternetDomanin
        = ./dnsenum -- enum internetDomanin
   return
   ListOfDNSserversOfInternetDomanin
}
```
(S5)

```
DeterminingNetworkRange(internetDomanin){
  dmitry -wnspb internetDomanin -o
  /root/Desktop/dmitry-result
  return dmitry-result.txt
}
```
(S6)

The next step consist of detecting the active servers from the system using the script (S7), the open ports for each server using the script (S8), identifying the operating systems on each server using the script (S9), and respectively detecting the services provided by each server using the script (S10), for NUMS fleets of Challenger and of the Defender, respectively [21], [22].

```
IdentifyingActiveMachines
(dmitry-result.txt){
  Define ActiveMachineList
  Foreach(IP address of  dmitry-result.txt)
  {
    ActivMachine = Nmap –sP IP
    Add ActiveMachine to ActiveMachineList
  }
  return  ActiveMachineList
}
```
(S7)

```
FindingOpenPorts(ActiveMachineIP){
  Define ActiveMachinePortsList
  ActiveMachinePortsList = Nmap
```
(S8)

```
  ActiveMachineIP
  Select only open ports of
  ActiveMachinePortsList
  return ActiveMachinePortsList
}

OperatingSystemFingerprinting
(ActiveMachineIP){
   Define
   ActiveMachineOSFingerprintingList
   ActiveMachineOSFingerprintingList = Nmap
   -O ActiveMachineIP
   return
   ActiveMachineOSFingerprintingList
}
```

(S9)

```
Servicefingerprinting(ActiveMachineIP){
   Define ActiveMachine
   Servicefingerprinting List
   ActiveMachine Servicefingerprinting
   List = Nmap -sV ActiveMachineIP
   return ActiveMachine
   Servicefingerprinting List }
```

(S10)

The combination of scripts (S11)-(S15) will provide information to the fleets about the active servers from the national cyber infrastructures of Challenger and Defender.

```
InformationGathering(InternetDomanin){
  ServiceEnumeration(internetDomanin)
  dmitry-result.txt =
  DeterminingNetworkRange(internetDomani
  n)
  ActiveMachinesList =
  IdentifyingActiveMachines
  (dmitry-result.txt)

  Define
    FindingOpenPortsListOfInternetDomain
    OperatingSystemFingerprintingListOf
    InternetDomain
    ServicefingerprintingListOfInternet
    Domain

  Foreach(IPActiveMachines of
  ActiveMachinesList){
    FindingOpenPortsItem  =
    FindingOpenPorts(IPActiveMachine)
    OperatingSystemFingerprintingItem  =
    OperatingSystemFingerprinting(IPActi
    veMachine)
  ServicefingerprintingItem =
  Servicefingerprinting(IPActiveMachine)
  FindingOpenPortsItem  Add
     FindingOpenPortsListOfInternetDomai
     n
     OperatingSystemFingerprintingItem
     Add
 OperatingSystemFingerprintingListOf
 InternetDomain
     ServicefingerprintingItem  Add
     ServicefingerprintingListOfInternet
     Domain
     }
   return
   FindingOpenPortsListOfInternetDomain
      OperatingSystemFingerprintingListO
      f InternetDomain
      ServicefingerprintingListOfInterne
      tDomain
}
```

(S11)

```
ServersListOfInternetDomain =
  Analyze nature of demons of
ServicefingerprintingListOf
InternetDomain and
OperatingSystemFingerprintingListOf
InternetDomain
```

(S12)

```
InternetDomainList = {
   Government,
   Military,
   Economy,
Social                    Media-Social
Network                        }
```

(S13)

The list of servers of each actor is given by (24) and (25).

```
InternetDomainListOfChallanger  =
ServersListOfInternetDomain of
Challanger's InternetDomainList
```

(S14)

```
InternetDomainListOfDefender =
ServersListOfInternetDomain of
Defender's InternetDomainList
```

(S15)

In order to determine the number of servers for 4 domains defined by (S13) script, the cardinal numbers of the sets defined by (S14) and (S15) scripts will be calculated.

$$n_{HTTPServers}^{Challenger} = card$$
{ InternetDomainListOfChallanger of HTTP Servers
}

(16)

$$n_{HTTPServers}^{Defender} = card$$
{ InternetDomainListOfDefender of HTTP Servers
}

(17)

Because the conflict between Challenger Defender takes place in an environment where very large amounts of information are circulating, it can be considered an information warfare, which controls large groups of UAV, UGV, and UUV-type mobile robots type using MANET networks. According to Poisel, the information warfare strategies can be reduced to four canonical strategists, generally each strategy being a result of their combination like a system of linear orthonormal vectors. The four canonical war strategists information are the following [4]:

- Disruption and destruction – consist of active denial of a reality by introducing false information in the system, which can lead to its destruction. A typical example is an aircraft jamming the tracking radar or the jamming of a MANET system, which leads some mobile robots.
- Subversion – uses the insertion of false information in the system, leading to start of a self-destructive process in the system. Examples are logic bomb systems, viruses, malware or destroying the control system by radio-electronic jamming / physical cyber-attack of a drone.
- Denial of information - consists of passive denial of a reality, such as the case of using stealth aircraft against radars. In the case of computer communication, one example is using encrypted communication or communication via VPN.
- Deception and mimicry – consists of inserting false information in the system (scanner). A typical case is an aircraft jamming the tracking radar. In the case of

computer communication, when scanning a network with NMAP, a computer sends also, besides the useful information, false information to the computer that scans the network.

By analyzing the above definitions, it can be concluded that the three primary cyber-attacks defined and grouped into two groups classified by macroeconomic costs, allow the organization of the cyber-attack classes to be completely defined as follows:

- To analyze Massive Cyber-Attacks implication, respectively Flexible Cyber-Attacks information warfare treated by bimatrix games with complete information, we use only two canonical strategies: Disruption and destruction, respective Subversion;
- To analyze Massive Cyber-Attacks implication, respectively Flexible Cyber-Attacks information warfare treated by bimatrix games with incomplete information, we use all four canonical strategies. In this case, we consider that mirroring of servers or alternative networks or encrypted channels are directly linked to the incomplete information of national cyber infrastructure.

Thus the relation between the two classes of cyber-attacks, the four canonical strategies of informational warfare and the information type is found in Table I:

TABLE I: THE RELATION BETWEEN TWO CLASSES OF CYBER ATTACKS

	Massive Cyber Attacks	Flexible Cyber Attacks	Information type
Disruption and destruction	software cyber-attack	software cyber-attack	Complete
	radio-electronic cyber-attack	radio-electronic cyber-attack	
	physic cyber-attack	physic cyber-attack	
Subversion	software cyber-attack	software cyber-attack	
	radio-electronic cyber-attack	radio-electronic cyber-attack	
	physic cyber-attack	physic cyber-attack	
Denial of information	Encryption and VPN communication		Incomplete
Deception and mimicry	Insert fake information in adversary computer network		

Once we have established a relationship between strategies of warfare information use and the two models of cyber-attack, then the calculation of utility functions according to the three costs defined by Gilpin, and the number of disabled servers through a particular strategy using relations (16)-(17), pre and post implementation strategies, are established. Thus, using the difference between the number of servers pre and post-attack for a particular size (military, economic, governmental, social networks), the value of the utility function is determined. Applying a multiple regression (suppose we have a sample of values for the number of servers of any size and, respectively, the Gilpin costs) according to the relations below, we establish the direct dependence of the number of servers on one dimension - Gilpin's costs:

$$\Delta n = f\left(\frac{\Delta x_{CNS}}{\Delta T}, \frac{\Delta x_{CPNP}}{\Delta T}, \frac{\Delta x_{CPI}}{\Delta T}\right) \tag{18}$$

and the inverse dependence of the number of servers on one dimension - Gilpin's costs:

$$\begin{cases} \dfrac{\Delta x_{CNS}}{\Delta T} = f_1^{-1}(\Delta n) \\ \dfrac{\Delta x_{CPNP}}{\Delta T} = f_2^{-1}(\Delta n) \\ \dfrac{\Delta x_{CPI}}{\Delta T} = f_3^{-1}(\Delta n) \end{cases} \tag{19}$$

The utility function is calculated as the below average:

$$U = \frac{\sum \Delta n_k}{N} \tag{20}$$

IV. RESULTS

Starting from organizing information warfare as bimatrix game, from the Nash solution of it we can deduce which is the proportion in which the actors use massive or flexible cyber-attack by checking the "The Gilpin Test".

In this study we considered only the case when information is complete and the game is reducible to only two canonical strategies: Disruption and destruction and Subversion. We believe that the game is a normal bimatrix game 2x2 characterized by the following utility equations [23]:

$$\begin{cases} U_{Defender} = (p,1-p)\cdot\begin{bmatrix} U_{D11} & U_{D12} \\ U_{D21} & U_{D22} \end{bmatrix}\cdot\begin{pmatrix} q \\ 1-q \end{pmatrix} \\ U_{Challenger} = (p,1-p)\cdot\begin{bmatrix} U_{C11} & U_{C12} \\ U_{C21} & U_{C22} \end{bmatrix}\cdot\begin{pmatrix} q \\ 1-q \end{pmatrix} \end{cases}$$

$$0 < p < 1,\ 0 < q < 1 \tag{21}$$

where U_{D11} – the utility function of Defender, when its strategies and the Challenger's strategies are Disruption and destruction - type; U_{D12} – the utility function of Defender when its strategy is Subversion – type and the Challenger's strategy is Disruption and destruction – type; U_{D21}- the utility function of Defender when its strategy is Disruption and destruction – type and the Challenger's strategy is Subversion – type; U_{D22}- the utility function of Defender when the strategy of both actors is Subversion

-type.

U_{C11}–the utility function of Challenger, when its strategies and the Defender's strategies are Disruption and destruction–type; U_{C12}–the utility function of Challenger when its strategy is Subversion – type and the Defender's strategy is Disruption and destruction – type; U_{C21}-the utility function of Challenger when its strategy is Disruption and destruction – type and the Defender's strategy is Subversion – type; U_{C22}- the utility function of Challenger when the strategy of both actors is Subversion -type.

For the above system, by applying the Lagrange multipliers, the below solutions for Nash point are obtained as follows [22]:

$$\begin{cases} p_0 = \dfrac{U_{C22} - U_{C21}}{U_{C11} - U_{C12} - U_{C21} + U_{C22}} \\ q_0 = \dfrac{U_{D22} - U_{D12}}{U_{D11} - U_{D12} - U_{D21} + U_{D22}} \end{cases} \quad (22)$$

$$U_{C22} > U_{C21},\ U_{C11} - U_{C12} - U_{C21} + U_{C22} > 0,$$
$$\left|U_{C22} - U_{C21}\right| < \left|U_{C11} - U_{C12} - U_{C21} + U_{C22}\right|,$$
$$U_{D22} > U_{D12},\ U_{D11} - U_{D12} - U_{D21} + U_{D22} > 0,$$
$$\left|U_{D22} - U_{D12}\right| < \left|U_{D11} - U_{D12} - U_{D21} + U_{D22}\right|,$$

Then the utility values in the defined Nash point will be [23]:

$$\begin{cases} U^0_{Defender} = (p_0, 1-p_0) \cdot \begin{bmatrix} U_{D11} & U_{D12} \\ U_{D21} & U_{D22} \end{bmatrix} \cdot \begin{pmatrix} q_0 \\ 1-q_0 \end{pmatrix} \\ U^0_{Challenger} = (p_0, 1-p_0) \cdot \begin{bmatrix} U_{C11} & U_{C12} \\ U_{C21} & U_{C22} \end{bmatrix} \cdot \begin{pmatrix} q_0 \\ 1-q_0 \end{pmatrix} \end{cases} \quad (23)$$

By applying the inverse dependence relation – number of servers on one dimension – Gilpin costs, the value of variation for the three Giplin costs is obtained for the cyber-attack period according to the following relations:

Defender's Gilpin costs:

$$\begin{cases} \dfrac{\Delta x^{Defender}_{CNS}}{\Delta T} = f_1^{-1}\left(U^0_{Defender}\right) \\ \dfrac{\Delta x^{Defender}_{CPNP}}{\Delta T} = f_2^{-1}\left(U^0_{Defender}\right) \\ \dfrac{\Delta x^{Defender}_{CPI}}{\Delta T} = f_3^{-1}\left(U^0_{Defender}\right) \end{cases} \quad (24)$$

Challenger's Gilpin costs:

$$\begin{cases} \dfrac{\Delta x^{Challenger}_{CNS}}{\Delta T} = f_1^{-1}\left(U^0_{Challenger}\right) \\ \dfrac{\Delta x^{Challenger}_{CPNP}}{\Delta T} = f_2^{-1}\left(U^0_{Challenger}\right) \\ \dfrac{\Delta x^{Challenger}_{CPI}}{\Delta T} = f_3^{-1}\left(U^0_{Challenger}\right) \end{cases} \quad (25)$$

Thus after we calculated the Nash point and determined the utilities of each of the players, we can determine which is the relationship among Defender, Challenger and the two models of massive and gradual attacks by checking the solutions of systems of equations above. Based on the verification of "The Gilpin Test" it will be determined which state is bankrupt and therefore defeated as it cannot continue the fight.

V. Future Works

This research is part of an extensive study of cyberattacks conducted using mobile robotic platforms. The system designed in this research represents the core of future developments where the direct/ indirect dependence functions - number of servers on one dimension - Gilpin's costs have also a spatiotemporal dimension for improving swarm intelligence algorithms such as Bat Algorithm, Artificial Fish Swarm, Cuckoo Search Algorithm, Firey Algorithm, Flower Pollination Algorithm, Artificial Bee Colony Optimization, Wolf-Based Search Algorithms, Bird's-Eye View. A second direction of future research is to study the behavior of a particular Challenger or Defender actor in case of an incomplete information environment endowed with four canonical strategies.

VI. Conclusion

Analyzing the elements presented in this research, the key concepts of our approach Massive Cyber Attack and, respectively, Flexible Cyber Attack have at this point a clearer and deeper approach. The two concepts are connected with three macroeconomic dimensions, cost for national security, public and private cost for nonmilitary and cost for productive investment. They indicate the economic state of the actor state and his motivation to choose for one of two mechanisms of cyber space attack using "The Gilpin Test". In the present research the use of games with complete information indicates which is the mix of the two types of attacks in reality by calculating the Nash equilibrium point and what would be the preponderance of the two in a process where a Challenger state cyber-attacks a Defender state. Another point of interest is the use of canonical strategies of information warfare, which have a great potential for future research in highlighting the elements of social engineering, cyber deception and counter-cyber deception in future approaches with all four strategies and incomplete information.

References

[1] H. Moga, M. Boscoianu, D. Ungureanu, R. Lile, and N. Erginoz, "Massive cyber-attacks patterns implemented with BDI agents," in *Proc. 6th International Conference on Aerospace, Robotics, Manufacturing Systems, Mechanical Systems, Mechanical Engineering, Biomechatronics and Neurorehabilitation*, vol. 811, October 2015, pp. 383-389.

[2] H. Moga, M. Boscoianu, D. Ungureanu, F. Sandu, and R. Lile, "Using BDI agents in flexible patterns for cyber-attacks over electrical power infrastructures,"

Applied Mechanics and Materials, vol. 841, pp. 97-104, June 2016.
[3] R. Gilpin, *War and Change in World Politics*, USA: Cambridge University Press, 1983, ch.4, pp. 159-168.
[4] R. A. Poisel, Information Warfare and Electronic Warfare Systems (Artech House Electronic Warfare Library), Artech House Publishers, 2013, ch.4, pp. 107-139.
[5] G. Dooly and E. Omerdic, "Unmanned vehicles for maritime spill response case study Exercise Cathach," Marine Pollution Bulletin, 110, pp. 528–538, 2016.
[6] Z. Liu and Y. Zhang, "Unmanned surface vehicles: An overview of developments and challenges," *Annual Reviews in Control*, vol. 41, pp.71–93, 2016.
[7] S. Karma and E. Zorba, "Use of unmanned vehicles in search and rescue operations in forest fires: Advantages and limitations observed in a field trial," *International Journal of Disaster Risk Reduction*, vol. 13, pp. 307–312, 2015.
[8] D. Axisa, T. P. DeFelice, "Modern and prospective technologies for weather modification activities: A look at integrating unmanned aircraft systems," *Atmospheric Research*, vol. 178–179, pp. 114–124, 2016.
[9] P. P. Neumann and S. Asadi, "Monitoring of CCS areas using micro unmanned aerial vehicles (MUAVs)," *Energy Procedia*, vol. 37, pp. 4182–4190, 2013.
[10] H. Kim, B. Kyeong Lee, and S. Y. Sohn, "Quantifying technology–industry spillover effects based on patent citation network analysis of unmanned aerial vehicle (UAV)," *Technological Forecasting & Social Change*, vol. 105, pp. 140–157, 2016.
[11] P. Papadakis, "Terrain traversability analysis methods for unmanned ground vehicles: A survey," *Engineering Applications of Artificial Intelligence*, vol. 26, pp. 1373–1385, 2013.
[12] I. Colomina and P. Molina, "Unmanned aerial systems for photogrammetry and remote sensing: A review," *Journal of Photogrammetry and Remote Sensing*, vol. 92, pp. 79–97, 2014.
[13] I. Sarıcicek and Y. Akkus, "Unmanned Aerial Vehicle hub-location and routing for monitoring geographic borders," *Applied Mathematical Modelling*, vol. 39, pp. 3939–3953, 2015.
[14] Jorayev and K. Wehr, "Imaging and photogrammetry models of Olduvai gorge (Tanzania) by unmanned aerial vehicles: A high-resolution digital database for research and conservation of early Stone age sites," *Journal of Archaeological Science*, vol. 75, pp. 40-56, 2016
[15] B. S. Faiçal, F. G. Costa, *et al*., "The use of unmanned aerial vehicles and wireless sensor networks for spraying pesticides," *Journal of Systems Architecture*, vol. 60, pp. 393–404, 2014.
[16] Y. Saleem, M. H. Rehmani, and S. Zeadally, "Integration of cognitive radio technology with unmanned aerial vehicles: issues, opportunities, and future research challenges," *Journal of Network and Computer Applications*, vol. 50, pp. 15–31, 2015.
[17] I. B.Tijani, R. Akmeliawati, *et al*., "Nonlinear identification of a small scale unmanned helicopter using optimized NARX network with multiobjective differential evolution," *Engineering Applications of Artificial Intelligence*, vol. 33, pp. 99–115, 2014.
[18] M. M. Tousi and K. Khorasani, "Optimal hybrid fault recovery in a team of unmanned aerial vehicles," *Automatica*, vol. 48, pp. 410–418, 2012.
[19] J. Y. Hung and L. F. Gonzalez, "On parallel hybrid-electric propulsion system for unmanned aerial vehicles," *Progress in Aerospace Sciences*, vol. 51, pp. 1–17, 2012.
[20] J. Wan, H. Suo, H Yan, and J. Liu, "A general test platform for cyber-physical systems: Unmanned vehicle with wireless sensor network navigation," *Procedia Engineering*, vol. 24, pp. 123–127, 2011.
[21] W. L. Pritchett and D. D. Smet, *Kali Linux Cookbook*, Birmingham: Packt Publishing, 2013.
[22] T. Heriyanto, L. Allen, and S. Ali, *Kali Linux: Assuring Security by Penetration Testing*, Birmingham: Packt Publishing, 2014.
[23] E. N. Barron, *Game Theory, An Introduction*, Second Edition, John Wiley & Sons, Inc., 2013, ch. 3, pp. 115-1731.

Horatiu Moga was born in Romania. He holds a PhD in Mechanical Engineering from Transilvania University of Brasov and currently he is Cyber Expert at National Agency for Fiscal Administration, Braşov and he is affiliated with Transilvania University of Brasov. He has a BS in Political Science at Lucian Blaga University Sibiu in 2000.

Mircea Boscoianu was born in Romania. Mircea Boscoianu holds a PhD in Cybernetics and Statistical Economics and PhD in Aerospace Engineering. He is Romanian Air Force Cdore and Professor at Henri Coanda Air Force Academy, Brasov.

Delia Ungureanu was born in Brasov, Romania, in 1957. She is graduated as Dipl. Eng. from the Faculty of Electrical Engineering, Transilvania University of Brasov, Romania, in 1981 and got his PhD in 2006 with a thesis on Distributed systems for process control with applications in thermo-energetic, from the Electrical Engineering and Computer Science Faculty of the Transilvania University of Brasov.

Before the academic career, she worked in designing automation equipment and software development in different Romanian companies. Since 2002 she has a university career with technical skills and competences in: design and implementation of integrated software systems; database management, expert systems, data mining and knowledge engineering, web programming, control and monitoring of industrial processes.

She is member of the Communications Society and member of the SRAIT – Romanian Society of Control Engineering and Technical Informatics, Brasov Branch.

Florin D. Sandu graduated as Dipl. Eng. from the Electronics and Telecom Faculty of Bucharest, in 1984 and got his PhD in 1998 with a thesis on Data Acquisition optimized for DSP, from the Electrical Engineering and Computer Science Faculty of the "Transilvania" University of Brasov. Before the academic career, he worked in the helicopter industry and since 2001 acts as consultant for Siemens Program and System Engineering Romania, managing the technology transfer towards the university and a set of joint EU-funded research common projects. Prof. Sandu is PhD coordinator, being also in charge with the curricular line in the telecom domain of the university. He is IEEE member of the Communications Society and member of the Romanian Society for Electromagnetic Compatibility.

Răzvan Gabriel Boboc was born in Brașov, in 1986. He received his Bachelor degree in Electrical Engineering, Telecommuncations specialization from Transilvania University of Brașov, Romania, in 2009. In 2011 he graduated Master program with specialization in Communication Networks. In 2015 he obtained the Ph.D. degree from Transilvania University of Brașov, Faculty of Mechanical Engineering with the thesis title "Natural human-robot interaction for assistive robotics applications". He is currently scientific researcher in the laboratory of Transilvania University of Brașov IIR (Industrial Informatics and Robotics), Department of Automotive and Transportation Engineering, where he makes education and research activities in the fields of Robotics, Human-Robot Interaction, Virtual Reality, Augmented Reality, 3D CAD Modeling, Computer Aided Design.