Modeling Conflicts Resulting from Sharing Telecommunication Resource between Antagonistic Control Systems

V Kh Fedorov\textsuperscript{1}, E G Balenko\textsuperscript{1}, Yu I Starodubtsev\textsuperscript{2}, E V Vershennik\textsuperscript{2}

\textsuperscript{1}Federal State Budgetary Educational Institution of Higher Education DON STATE AGRARIAN UNIVERSITY
pos. Persianovsky, 346493, Russian Federation
\textsuperscript{2}FGKVOU VPO "Military Academy of communications named after Marshal of the Soviet Union S. M. Budyonny»,
St. Petersburg, 143900, Russian Federation

E-mail: balenko2008@mail.ru, Yelena.Vershennik@mail.ru

Abstract. Today state-of-the-art communication systems, whilst being limited in resources, use a shared information and telecommunication network to provide integrated communication services; the resources of such a network are split between various control systems, some of which may conflict, resulting in a variety of malware attacks. This paper dwells upon a method for modeling conflicts resulting from sharing a telecommunication resource between antagonistic control systems; the method takes into account the use of such a shared resource (ITCN) and the following processes: data processing by cyber threat intelligence systems, and making decisions on executing MAs upon the elements of conflicting control systems; for each moment of simulation time, the method calculates the current potential of each conflicting system in order to find the average potential degradation time.

1. Introduction
Communication systems form the backbone of control systems. Earlier, each control system would only engage its own communication system. However, wide adoption of multiservice networks resulted in a transition from separate communication services (phone, telegraph, data transmission, etc.) to integrated services. Today’s services such as VoIP, video conferencing, etc. require more bandwidth and higher service quality. Thus, being limited in resources, control systems need to use a shared resource (the information and telecommunication network); when antagonistic systems share a resource, various actions may occur [1].

2. Analysis of the existing conflict modeling methods
Today’s research is focused on creating simulation modeling tools and methods as part of decision support frameworks, including conflict resolution toolkits [2 - 6].

Thus, there are systems that can model bilateral combat action involving heterogeneous groups; they can simulate various scenarios of suppressive fire against single entities or groups; they can also evaluate the combat potential of armaments. However, these systems and methods only take into account combat potential, which is derived from the availability of armed forces and weaponry; they
cannot simulate information potential and what the communication system contributes to the superiority of either party in combat.

Yet, analysis of the conflicts of recent decades shows that they also take place in the information and telecommunication environment, where they affect not only the elements of the communication system as part of a broader control system, but also the data it stores and transmits, including metadata; element status data; and functioning algorithm data, etc. [7, 8].

Papers [9-11] detail upon modeling conflicts in information and telecommunication space and in cyberspace. However, the implementations covered therein do not take into account the fact that antagonistic control systems may share a resource, the information and telecommunication network; those methods cannot simulate bilateral cyber threat intelligence processes that affect control and communication systems; nor can they simulate malware attacks (MA). They are not capable of accurate and reliable calculating of the average time for the parties-in-conflict’s potential, including the information potential, to degrade.

3. Modeling conflicts resulting from sharing a telecommunication resource between antagonistic control systems: statement of problem

When conflicting control systems share a single telecommunication resource, intelligence data gathered by cyber threat intelligence in order to plan attacks on, and to compromise communication systems, becomes crucial. Such attacks can target not only the communication systems of the enemy, but also the shared information and telecommunication network. Malware attacks are the main course of impact.

Therefore, there is a need to model conflicts by a method that could simulate bilateral effects that antagonistic control systems could have on each other when sharing a single information and telecommunication network section, which includes simulation of cyber threat intelligence processes; such methods should also be capable of modeling malware attacks and calculating with sufficient accuracy and reliability the average time for the parties-in-conflict’s potential, including their information potential, to degrade.

Below are the key limitations and assumptions:

1. The solution will ignore any attacks that do not rely upon an array of up-to-date, complete, and accurate data about the target; this means each of the parties-in-conflict can be modeled as a trio of interrelated systems: data retrieval, data processing, and data implementation.

2. Attacks can be launched from any part of the information and telecommunication space, although element-specific limitations apply.

3. All targets are potentially vulnerable to a multitude of various threats.

4. Targets are stationary.

4. Modeling conflicts resulting from sharing a telecommunication resource between antagonistic control systems: the method

Stage 1. Preparing input data [12].

Implementation of the proposed method requires the following input data:

- data on the conflicting control and communication systems: what they are composed of, how they are structured and placed in the area in Cartesian coordinates, and specifications of their elements;

- data on the public communication network that serves as the shared telecommunication resource: what it is composed of, how it is structured and placed in the area in Cartesian coordinates, and specifications of its elements;

- number of attack targets, their placement in Cartesian coordinates. Attacks can target control and communication system facilities, elements of the public communication network, facilities of governmental agencies, critical IT infrastructures, etc.

- performance specifications of the targets;

- initial information and combat potential of each control system engaged in conflict \( K_{ij} \);
- minimum information and combat potential the reaching of which will mean a loss for a conflicting control system;
- the required accuracy and reliability of calculating the average time for the conflicting control systems’ information and combat potential to degrade;
- number and specifications of malware attack tools, the periodicity and intensity of such attacks.

Malware attacks (MA) are defined herein as any action that an antagonistic software control system can execute in order to alter the composition, structure, and functioning of the information and telecommunication network elements or a set thereof. Typical MAs include denial of service, DOS attacks, ping attacks, address spoofing, etc. [13,14].

These inputs can be collected by pre-measuring these parameters, calculating the initial resources available to the conflicting control systems, and estimating the effects of key attacks on various targets on a specific timeframe.

For the model to be sufficiently accurate, find the required number of experiments n.

To find the required number of tests, one can use the following formula based on normal approximation to the binomial:

\[ n = \frac{p'(1-p')}{E^2} Z^2 \frac{a}{2} \]

where \( E \) is the maximum permissible error of estimating \( p \);
\( 1 - a \) is the confidence limit or the desired probability of the estimated \( p' \) not differing from \( p \) by more than \( \pm E \);
\( p' \) is the initial estimate of \( p \);
\( Z^2 \frac{a}{2} \) is the \( 1 - \frac{a}{2} \)th point of the normalized normal distribution.

Assuming the sampled values from the general population are distributed normally, we can now show that

\[ n = \left( \frac{\sigma a}{d} \right)^2, \]

where \( \sigma \) is the variability of the population;
\( Z^2 \frac{a}{2} \) is the permissible risk value;
\( d \) is the permissible difference between the estimate and the actual value of the parameter [16, 17].

Beside, this is the time to set \( \Delta t \), which is a step of the current simulation time.

Such a step can be set as a fixed step, a step to the next event, or as a variable interval. In case of a fixed time step, system time is counted in predetermined constant time intervals. In case of step to the next event, each new significant event triggers system status update regardless of the time between the events [17]. In case of variable time step, system time is counted in variable time intervals determined as described in [17, 18].

**Stage 2.** Modeling the physically and logically interacting section of an information and telecommunication network (ITCN) shared by conflicting control systems; simulating the functioning of such systems.

Methods described in [19-25] can be used to model the physically and logically interacting section of an information and telecommunication network (ITCN) shared by conflicting control systems, and to simulate the functioning of such systems.

**Stage 3.** Modeling data retrieval as performed by cyber threat intelligence (CTI) through channels and tracts of a public communication network shared between conflicting control systems.

Cyber threat intelligence is an activity that seeks to retrieve data from computer databases connected to open networks, and to collect data on the structure and functioning of the systems that host such databases.
Cyber threat intelligence intends to collect data on conflicting control systems, communication systems, outputs, forms and methods of the parties-in-conflicts’ activity that engages a shared technological resources (the ITCN), hardware and software in use, control and information exchange protocols, and protections in place.

Intelligence data is collected by computer hardware and software that runs logical operations and techniques.

Data collection methods and processes are covered in [13,14,26] and include such operations as planning, targeting, and data retrieval.

Planning includes defining the key objectives of data collecting, the need for information, possible sources of data for each particular objective, and the means available to CTI, whether they are regularly available or could be requested additionally.

Data retrieval and collection involves using the means to obtain data from a variety of sources and collection of such data by the designated subsystems of the conflicting control systems.

Stage 4. Modeling data processing for either conflicting control system.

Cyber threat intelligence is tasked to collect and process data. Data processing generally involves operations that can be classified as inventory, sampling, verification, and evaluation [13, 14, 26].

Inventory (systematization) is defined as classification and systematization of data by the commonality of topics; data is source- and time-stamped.

Sampling involves finding and isolating information that pertains to this or that particular objective.

Verification is defined as analysis intended to check the authenticity, truthfulness, correctness, source reliability, time since retrieval, accuracy, and reliability of data compared to the preliminarily available information.

Evaluation consists in estimating the following parameters of data:
(a) quality:
- reliability (correctness) of information;
- reliability of the source;
- unambiguity;
- number of ‘middlemen’ between the original source and the recipient of data;
(b) quantity:
- completeness of data, i.e., the extent, to which it is in line with the targets of intelligence;
- relevance of data, i.e., the extent to which it is in line with the essence of the problem being solved or with the objectives of intelligence (represented as % of the total data);
(c) value:
- cost of data, i.e., the costs of obtaining it;
- relevance of data, i.e., the time during which these estimates remain up-to-date.

Stage 5. Modeling decision making on MAs against elements of the conflicting control systems.

Decision-making is essentially finding the situation-optimal behavior strategy [13, 14, 26]. Making a decision on executing MAs against elements of the conflicting control systems involves isolating a finite set of MAs that will target the opposing conflicting system, choosing an MA model, and selecting targets to reduce or eliminate the potential of the opposing control system.

Paper [13] highlights the following malware classes: computer viruses, worms, trojans, backdoors, and implants.

MAs can use the following models:
- Interception. Malware is injected into the operational environment to intercept and copy target data;
- Trojan. Malware is embedded into continuously running software or service for the purpose of information theft;
- Observer. Malware is embedded into continuously running software or service and monitors information processing. It can also control further MAs;
- Distortion or error initiation. Upon triggering in a computer system, malware distorts the output stream, spoofs inputs, initiates or suppresses application errors;
- Copying data fragments to external storage;
- Tampering with application algorithms;
- Blocking certain application modes.

MAs can target facilities of conflicting control systems directly; alternatively, they can affect the shared resource, the ITCN, as causing a blackout of specific elements may compromise the potential of the opposing control system.

It should be borne in mind, however, that, since the control systems share a single telecommunication resource, some ITCN elements may be servicing both parties. For that reason, when simulating the functioning of control systems and the communication systems they use, one needs to detect data routes of the corresponding pairs and isolate the ITCN elements used by the parties-in-conflict. These elements should either be excluded from the list of MA targets; alternatively, their parameters could be modified for a specific timeframe.

Paper [27] presents an overview of how ITCN attacks of the warring parties could be modeled.

Stage 6. Estimating the current potential of each conflicting control system.

The current potential of each conflicting control system for each moment of simulation time can be calculated as follows

\[ K_{ij}' = K_{ij} - \Delta K_{ij}, \]  

where \( i \) is the number of conflicting control systems; \( j \) is the number of targets for each conflicting control system; \( K_{ij} \) is the initial potential of each conflicting control system; \( \Delta K_{ij} \) is the losses of each conflicting control system.

Calculated current potential of each conflicting control system is then compared against the set minimum. If the current potential > minimum potential, run the model further. If the current potential of a single conflicting control system \( \leq \) minimum potential, find the average degradation time with the required accuracy and reliability. To find the average potential degradation time \( (\overline{T}) \), use sample mean:

\[ \overline{T} = \frac{1}{n} \sum_{i=1}^{n} T_i, \]  

where \( n \) is the required number of experiments for each conflicting control system; \( T_i \) is the potential degradation time in the \( i \)th experiment.

5. Conclusions
Thus, the method presented herein takes into account the use of such a shared resource (ITCN) and the following processes: data processing by cyber threat intelligence systems, and making decisions on executing MAs upon the elements of conflicting control systems; for each moment of simulation time, the method calculates the current potential of each conflicting system in order to find the average potential degradation time. Russian Invention Patents certify the novelty and practical significance of the proposed solution.

6. References
[1] Starodubtsev Yu I, Chukarikov A G, Korsunsky A S, Sukhorukova E V 2016 Principles of safe use of communication infrastructure in relation to the conditions of technosphere war In the collection: Integrated control systems, collection of scientific papers of the scientific and technical conference pp 199-206
[2] Semenov S S, Gusev A P, Barbotko N V 2013 Assessment of the information and combat potential of the parties in technospheric conflicts Science-intensive technologies in space research of the earth 6 pp 10 - 21
[3] Burenok V M, Tsirendorzhiev S R 2013 Creation of a modeling system is a necessary condition for the development of the RF Armed Forces Armament and Economics 4 pp 4 - 11
[4] Buravlev A I, Brezgin V S 2013 Methodology for assessing damage in the simulation of fire damage to an object Armament and Economics 4 pp 13 - 21
[5] Brezgin V S 2009 Methodology for calculating the combat potentials of weapons and military equipment based on the results of simulation of combat operations Armament and Economics 1 pp 31 - 34
[6] Buravlev A I, Gordeev S V 2009 Model of the dynamics of the confrontation between heterogeneous groupings of forces 1 pp 13 - 26
[7] Starodubtsev Yu I, Zakalkin P V, Ivanov S A 2020 Technosphere War as the Main Way of Conflict Resolution in the Context of Globalization Military Thought 10 pp 16-21
[8] Starodubtsev Yu I, Semenov S S, Bukharin V V 2010 Technosphere War”, scientific and technical journal "Bulletin of the Military University" (M. : Science-XXI) 4
[9] Starodubtsev Y I, Vershennik E V, Balenko E G, Fedorov V H 2020 Method for simulating conflict situations in cyberspace In the collection: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) p 9271648
[10] Alasheev V V, Vershennik A V, Vershennik E V, Latushko N A, Starodubtsev Yu I, Chesnakov M N 2017 Patent 2662646 Russian Federation G06N 5/00 (2006.01), G06F 17/30 (2006.01) A way of modeling conflict situations 2017137709 declared 10/27/2017 bull 21 p 17
[11] Belov A S, Budilkin S A, Starodubtsev Yu I, Grechishnikov E V, Alisevich E A 2006 Patent 2440611 Russian Federation, IPC G06N 5/00 (2006.01) A method for modeling bilateral impacts applicant and patentee Federal State Budgetary Educational Institution of higher professional education Academy of the Federal Security Service of the Russian Federation (Academy of FSO of Russia) 2010126509/08 app. 06/28/2010 publ. 20.01.2012 bull 2
[12] Brechko A A, Vershennik A V, Vershennik E V, Lvova N V, Pervov M S, Starodubtsev Yu I 2019 Patent 2708354 Russian Federation, H04L 9/002 (2019.05), H04K 1/00 (2019.05), G09C 1/00 (2019.05) A method for modeling bilateral impacts using conflicting control systems of a common technological resource 2018122181 declared 06/15/2018 published on June 24 2019 bull. No. 18 - 17 p 3
[13] Starodubtsev Yu I 2017 Quality management of information services under total Ed Yu I Starodubtseva (SPb. : Publishing house of Polytechnic. University) 454 p
[14] Shangin V F 2017 Information security of computer systems and networks: textbook. allowance (Moscow: Publishing house FORUM: INFRA-M) 416 p
[15] Menshakov Yu K 2017 Fundamentals of protection against technical intelligence (М. : IPC "Mask") 572 p
[16] Khan G, Shapiro S 1969 Statistical models in engineering problems (М. : Publishing house "Mir") pp 280-283
[17] Shannon R 1978 Simulation system - art and science (М. : Publishing house "Mir") pp 213-220
[18] Sukhorukova E V, Zakalkin P V, Andreyanov S N 2013 Modeling of trade business processes: methods of setting the model time Problems of Economics and Management in Trade and Industry 1 pp 104-109
[19] Alisevich E A, Evgrafov A A, Nizhegorodov A V, Starodubtsev Yu I, Sukhorukova E V 2013 Patent 2541169 Russian Federation, IPC G06N 99/00, G06G7 48 System for modeling dynamic processes applicant and patentee Federal State Budgetary Educational Institution of Higher Professional Education "St. Petersburg State University of Trade and Economics” 2013108784 declared 02/26/2013 publ. 02/10/2015 bulletin 4 - 17 p
[20] Galkin A P 1979 Modeling of communication systems channels (М. : “Communication”) pp 40-45
[21] Vershennik E V, Balenko E G, Zakalkin P V, Fedorov V H 2020 Communication Network Modeling Taking Into Account Different Kinds Of Inhomogeneities In: 2020 International Multi-Conference on Industrial Engineering and Modern Technologies (FarEastCon) p 9271525
[22] Alisevich E A, Sinev S G, Starodubtsev P Yu, Sukhorukova E V, Chukarikov A G, Sharonov A N Patent 2546318 Russian Federation, IPC G06F 17/10 (2006.01), G06F 17/50 (2006.01), H04W 16/22 (2009.01). A method for modeling communication networks applicant and patentee Federal State Budgetary Educational Institution of Higher Professional Education “St. Petersburg State University of Trade and Economics” 2014103873 declared 02/04/2014 publ. 10.04.2015. bul. pp 10 - 21

[23] Alisevich E A, Zakalkin P V, Kirillova T V, Starodubtsev Yu I, Sukhorukova E V, Chukarikov A G 2015 Patent 2562767 Russian Federation, IPC G06N 5/00. A way to adaptively improve the adequacy of the model applicant and patentee Federal State Budgetary Educational Institution of Higher Professional Education “St. Petersburg State University of Trade and Economics” 201411876 declared 03/27/2014 publ. 09/10/2015. bul. No. 25 14 p

[24] Anisimov V V, Begaev A N, Starodubtsev Yu I, Sukhorukova E V, Fedorov V G, Chukarikov A G 2017 Patent 2620200 Russian Federation, IPC G06N 5/00 (2006.01) H04W 16/22 (2009.01) G06F 17/10 (2006.01) The method of purposeful transformation of the parameters of the model of a real fragment of a communication network applicant and patentee Begaev A N 2016119980 declared 05/23/2016 publ. 05/23/2017. bul. No. 15 p 18

[25] Belikova I S, Zakalkin P V, Starodubtsev Yu I, Sukhorukova E V 2017 Modeling of communication networks taking into account topological and structural inhomogeneities Information systems and technologies 2(100) pp 93-101

[26] Baburin A V, Chaikina E A, Vorobieva E I 2006 Physical bases of information protection from technical means of intelligence: Textbook. allowance (Voronezh: Voronezh. state tech. un-t) 193 p 8

[27] Brechko A A, Bukharin V V, Vershennik A V, Vershennik E V, Lvova N V, Starodubtsev Y I 2017 Patent 2655466 Russian Federation, G06N 5/00 A method for modeling deliberate damage to elements of a communication network operating in the interests of heterogeneous, including antagonistic control systems applicant and patentee 127332 declared 07/31/2017 published on May 28, 2018. bull. No. 16 14 p