# RATIONAL CHOICE AND CYBERSECURITY

**Ph.D. Student, Mihaela Hortensia HOJDA**
"Valahia" University of Târgoviște, Romania
E-mail: hmihaelah@gmail.com
**Professor habil. Ph.D., Mihai MIEILĂ**
"Valahia" University of Târgoviște, Romania
E-mail: m_mieila@yahoo.com
**Dipl. Eng. Ph.D., Cristian MIEILĂ**
University Politehnica of Bucharest, Romania
E-mail: cristian.mieila@gmail.com
**Ph.D. Student, Liviu Constantin DAFINA**
"Valahia" University of Târgoviște, Romania
E-mail: liviudafina@yahoo.com

***Abstract:*** *Along the technological development of recent years, cyber threats have become increasingly common. Cyber threats can target both the devices of individuals, but especially critical objectives related to digitized objectives within the national industry, namely power plants, public services, government agencies, health system or vital private services, such as the banking system. Thereby, cyberspace has become an operational space, under the statal authority, in terms of ensuring security. With the expansion of digitalization in more and more application areas, cybersecurity has become a vital aspect of national security, aimed to protect individuals and infrastructures or services of national importance. Due to the increased importance of cybersecurity, the paper starts from the assumption that the state, as a rational actor, is the ultimate agent in terms of ensuring security, and examines the ways in which the state can address cyber threats. In this respect the rational choice theory, represents a topical approach. Namely, the state, as an individual actor, can adopt a rational conduct regarding prevention, response, and recovery after a cyberattack. Rational choice theory can be a good guide for outlining a choice in terms of the existence of two or more alternatives in an environment determined by information volatility.*

***Keywords:*** *rational actor, cybersecurity, rational choice theory.*
***JEL Classification:*** *O33*.

## 1. Introduction

In the context of technological development in recent years and specific means in the cyber field, this area has acquired an increasing importance. With the expansion of the fields of applicability of cyberspace, from the small space applicable first to military infrastructures to civilian ones, to almost all important spheres of public or private life, the need for cyber security has become more and more pressing.

Currently, in the military space, the cyber domain shows its usefulness, but also its lethal component, in the confrontations within the war in Ukraine, which generates an accelerated progress in all technological areas specific to the war. Also, in recent decades, more and more critical areas have been digitized, which, in addition to the multiple advantages brought by digitization, has also come with the related cybersecurity risks. This can include hospitals, government structures, certain objectives of strategic interest, such as energy sources and so on, which are potential targets for hackers. As proof of the importance of this critical area of cybersecurity, NATO itself introduced cyberspace in 2016 among the other three operational spaces (air, sea, land), subject to Article 5 of the Alliance treaty, turning it into a battlefield (NATO, 2023).

Thus, the battlefield is no longer reserved only for classical means, seen, represented by armies, but also for less detectable ones, such as cyber. Given the increasing importance in

recent years of the field subsumed by cyber security, as a critical field, this paper starts from the assumption that the state, as holder of the legitimate monopoly on coercion, is the court under whose authority falls the responsibility to manage and respond to cyber threats. On the other hand, this raises the legitimate question of how the state can address cyber threats. One answer to this is given by rational choice theory. Namely, the state, as an individual actor, can adopt a rational conduct regarding prevention, response and recovery after a cyber attack.

This theoretical approach is one with a long tradition and represents one of the most well-known and used approaches in political science, proving to be useful in decision-making processes at the state level. On the other hand, the adornment represented by the theory of rational choice is also a good guide from a theoretical point of view to state action in the field reserved for security, today extended to cyberspace. Next, the work is divided as follows. A first part aims to present the rational choice paradigm, a second part refers to the integration of rational choice in cybersecurity, and the last part is reserved for conclusions.

**2. The paradigm of rational choice theory**

This section has the role of making a foray into the paradigm represented by the theory of rational choice (TAR), in order to extract a useful meaning for the present research, applicable to the field represented by cybersecurity. From the outset, we must exclude the common, scientifically unsubstantiated meaning, which refers to a person's ability to use his cognitive functions to act, that is, reason in the sense of a simple act of thinking. As the name of this theory derives, reason, or cold calculation, without subjective emotions and passions, is the element that constitutes the lifeblood of this approach. It has both an explanatory component - "why do individual entities act in a certain way?" - and a normative, prescriptive component - "how should an individual entity (the state, in this case) act to best pursue its interests?".

If goals or interests are the result of a subjective process of cognition and definition, means or even ends can be subjected to a process of rational coagulation, according to well-established criteria. Given the individualistic side of this paradigm, applied in the field of state decision, this paper will use the assumption that the state is an individual actor, to whom the attribute of rationality is attributed. In short, the state is a rational actor. In the following lines, this section will be reserved for presenting the most important concepts belonging to the paradigm of rational choice, which are based on a sum of specific principles.

As a theoretical paradigm, rational choice theory refers to phenomena that shape social choice, which is reserved for individuals, supposedly rational, thus trying to give meaning to behaviors starting from real situations (Miroiu, 2006, p. 20). Hence the assumption that the sum of individual actions is the basis for the totality of social phenomena or decisions, doubled by a second premise, which assumes the rationality of individuals (Miroiu, 2006, p. 24).

Rational choice theory has deep roots in economics, where reason and egoism are defining characteristics. The first characteristic calls for the elimination of emotions from the actional sphere through the use of objective and logical thinking, while the second requires a focal point focused on gain, in any circumstance, disregarding others. Neoclassical economics is based on these two components in explaining behavior at unit level, in conditions of insufficiency (Ungureanu, 2018, pp. 19-20).

Within the TAR perspective, the term "rational" is circumscribed an instrumental meaning, hence the term "instrumental rationality", which designates the way in which

individuals pursue certain goals derived from their own desires and preferences. The goals are thus achieved through specific instruments, meant to outline the individual action - rational-instrumental - in order to better achieve the goals (Miroiu, 2006, pp. 35, 38-39; Simon, 1983, pp. 7-8; Grünberg, 1989, p. 162).

According to Max Weber, instrumental rationality relates to how objectives can be achieved, starting from the assumption that the action of individuals is by itself rational (Miroiu, 2006, p. 38; Weber, 1978, p. 25). Or, in the words of a classic author, John Stuart Mill, "[t]he [e]xist [...] a large class of social phenomena whose immediate causes are principally those acting by the desire for wealth, and for which the psychological law implied is the familiar one according to which the greater gain is preferred to the less" (Mill, 1843, p. 878).

Three principles underlie instrumental rationality, namely: Principle of effective means, Principle of comprehensiveness and The principle of higher probability (Miroiu, 2006, p. 39; Rawls, 1971, pp. 411-413). The principle of effective means is par excellence the model of the classical homo economicus, that is, the individual who has preferences and the context of choice, acting with all means for the optimal realization of self-interest (Buchanan and Tullock, 1962, p. 33; Miroiu, 2006, pp. 40-41).

Instrumental rationality is distinguished in two ways of definition. The first is rationality as internally consistent choices, which refers to an individual's decision in the context of group membership, then to the relevance of this decision for the group in question, as well as how to influence the decision of the group outcome, but also how the group influences the individual decision in reverse. This makes the decision not dependent on a single individual in the group. The second way refers to rationality as maximization of self-interest, where each individual in the group is reserved a sum of alternatives, assessable according to benefits, while also taking into account that the other members of the group are in the same situation. In this case, individual action also relates to the mode of action of the other individuals of the group (Miroiu, 2006, pp. 43-44; Sen, 1987, p. 12).

According to Adrian Miroiu, the rational individual possesses three attributes. First, it possesses perfect rationality, which determines the ability to choose between alternatives, compare and rank to choose the best alternative. Second, the rational actor acts by pursuing a self-interest And he doesn't aim for what he does to help others, but also not to harm them. Third, the rational individual owns perfect information, that is, the totality of information needed to choose favorably (alternatives, rules, existence of individuals with similar possibilities) (Miroiu, 2006, pp. 41-42).

The *MaxiMin* principle of action represents another important decision-making component that characterizes a rational actor. According to John Rawls, in an initial situation, in the process of designating social rules, people will not want to take risks (Rawls, 1971). The maximin principle thus involves choosing the least possible evil, not necessarily the best outcome, being specific to the homo economicus pattern. Rawls stated that maximin requires probabilistic calculations under uncertainty, the desirable alternative being the one with the highest possibility of realization, with minimal risks (Miroiu, 2006, pp. 48-49; Rawls, 1971, pp. 154-155). According to this principle, the individual compares all available alternatives and chooses the safest and plausible one (Nurmi, 1983, p. 186).

Coming from the sphere of International Relations, John J. Mearsheimer appreciated states as rational actors. In fact, the rationality of actors, of states in this case, represents a fundamental assumption of realism as a paradigm, from which Mearsheimer comes.

According to him, states know the outside world, on which they have a strategic approach, analyzing their preferences and behaviors in relation to those of other states, to predict how their actions can be influenced. States have both a short- and long-term approach to their own behavior. In conditions of systemic anarchy (there is no hierarchical authority above states in the international system), states, especially great powers, possess capabilities through which they can cause damage to others, never having certainty about the intentions of others, whether they can be aggressive or not. Thus, in the international system, states operate under conditions of uncertainty, of imperfect information (Mearsheimer, 2003, p. 27).

For Mearsheimer, rationality involves striving to understand the world around us in order to achieve foreign policy goals, by the best means, within the framework of a credible theory (Mearsheimer and Rosato, 2023, p. 2). Moreover, both decision-makers and states taken as a unit operate in an international environment where information is scarce, non-existent or uncertain, at the level of their own state, friends or enemies (Mearsheimer and Rosato, 2023, pp. 4-5).

Other relevant contributions to the field of rational choice theory were made by Christopher A. Sims and Thomas Sargent, winners of the Nobel Prize in economics in 2011. According to Sims, Goldfeld and Sachs, in economics, the assumption of rational expectations, used in policy analysis, states that, according to its own objectives and available information, the public adopts optimal behavior, understanding exactly the path chosen for implemented policies, whether present or future actions (Sims et. al, pp. 111-112). Also, according to Sargent and Wallace, public expectations will vary depending on the policy regime. Concurrently, public expectations will change with policies if perceptions are accurate (Sargent and Wallace, 1974, pp. 7-8). In his turn, Nicholas Georgescu-Roegen advanced a theory - the law of entropy - according to which the natural resources of the Earth are finite, to be exhausted in the end, as a result of human consumption (Georgescu-Roegen, 1974).

In conclusion, the rational actor, in this case the state, is represented by an entity that makes decisions in a strategic manner, according to self-defined goals, making use of the means at its disposal and seeking to maximize its interests. The rational actor outlines a hierarchy of interests, proceeding to maximize them, to make the best choice.

### 3. Integrating rational choice into cybersecurity

Cyberspace is a constantly expanding field, with the digitization of more and more fields, from financial-banking, government, hospitals or other critical infrastructure, but especially the military field. Thus, they become targets for hackers, whether they belong to a state or a non-state organization, being attackable, with damage that can be comparable to that caused by kinetic attacks, such as bombings. The destruction is not similar to that generated by bombing, but it can temporarily stop the activity of certain critical targets. Moreover, if in the case of a bombing, for example, most of the time the source of the attack is known, in the case of a cyberattack often the origin of the source is diffuse, and some states may even deny involvement. From the start, the level of information may be lower, because there is a possibility of not detecting the source of the attack, which means that the level of uncertainty in which it is operated is higher.

One cannot overlook a foray, at least minimal, into the meanings that the concept of "cyber security" requires. What is cybersecurity about? What does it protect? It aims to secure data and refers to the defense of computer systems and users, through a sum of guarantees and

measures, against attacks, damage or access from unauthorized sources. It also involves prevention or detection, response and recovery in case of cyber incidents.

Cybersecurity operates on two distinct levels. The first refers strictly to security and protected values, while a second layer refers to the more modern field designated by information technology (IT) and cybernetics, an autonomous domain and subject to continuous changes. Some theorists consider different angles of reporting on cybersecurity. For example, von Solms and van Niekerk give a narrow meaning to cybersecurity, pointing out the existence of a distinction of cyber security - information security, the second type being embedded in the first, by involving individuals, processes and technology (von Solms and van Niekerk, 2013). However, Kianpour, Kowalski and Øverby (2021) argue that "cybersecurity deals with the various procedures that create a secure environment by protecting assets".

As mentioned earlier, this paper assumes that the ultimate depository of the decision regarding the management of cybersecurity is the state, in a Weberian sense, as the holder of the monopoly on legitimate coercion. Another argument is related to the fact that national defense policy falls under the responsibility of the state, which must develop the main decision-making and procedural tools, as well as optimal capabilities to ensure prevention, response and recovery in case of cyber attack. In this respect, the state, through the agency or agencies managing cyber security issues, acts according to a unitary, individual actor.

An important aspect regarding state action in the field of cyber security is related to the space defined by volatility and information uncertainty. According to the precepts of rational choice theory, the individual decision-maker must have all the information necessary to make the best decision. This is more difficult in cyberspace, where the threat and its source are less visible than, for example, airspace, land or sea, where sources and means of attack are more visible and easier to detect, thus also making it easier to respond or provide protection than in cyberspace.

As well as air, land or sea threats, the effect is amplified by anarchy within the international system, which implies the lack of a central authority over states. Thus, states must ensure their own protection against cyber threats. In case of attack from an external source - another state or a non-state entity - the individual state cannot address a higher authority, as is the case in the hierarchical environment of domestic politics.

Starting from the principle of instrumental rationality, I assume that the state is an individual actor. The state assumes the objective of ensuring national security, targeting all spaces, namely land, air, sea and, more recently, cyber. Adopting the homo economicus principle, the state, as an individual unit with preferences and the context of choice, must act using all means for the optimal realization of its own interest, which is to ensure the cyber security of the vital objectives concerned. The means that can be at the disposal of the state to ensure cyber security can be policies, strategies, decision-making procedures, regulations, hardware or software equipment, human or financial resources, resources that must be allocated in the most efficient manner.

Nor should we lose sight of the fact that, within an international system of an anarchic character, the state must also take into account other international actors, state or non-state, such as hacker groups or transnational terrorist organisations, which have an offensive potential. Not only does the state in question have its own capabilities, which it may not know or estimate exactly, but also the other states have certain capabilities, which they can use to pursue their own interests, more or less offensive. Thus, in shaping the decision, the state

must take into account that it does not operate in a vacuum, that there are other actors around it, with their own capabilities, about which it may not have complete or accurate information. Therefore, information is not perfect, but interests in a multi-entity world must be pursued, having a certain amount of information at their disposal, given the possession of a quantity of finite means, which must be allocated efficiently.

If reference is made to internally consistent choices, which assume that an individual's decision is made taking into account group membership, being relevant to the group in question, the state entity responsible for ensuring cybersecurity at the level of society must adopt decisions in the context of the reference group or groups - the decision group (advisors, subordinates), state agencies, and perhaps even society more broadly. Thus, decisions to ensure cybersecurity within a company are the result of group deliberation, relevant at the level of the reference group. This way of making decisions may be rather specific within democratic societies, where political decision-making envisages a process of deliberation, group coercion, as well as a process that takes into account the influence of public opinion, which means that decision-makers must bear in mind that some measures (restrictions, prohibitions, etc.) may be unpopular.

Regarding rationality as maximization of its own interest, the state, as a component of the group designated by the international system, populated with other entities with different, even opposite, interests, has at its disposal a sum of alternatives, which it can subject to an evaluation process taking into account the benefits it can bring, in relation to other international actors. A rational approach is for the state to maximize its own interest, given the existence of other actors in the international system, with their own interests, which they can pursue in a similar manner. The other actors may have practices or policies similar to the State concerned, similar interests, smaller or broader in scope. The other actors may also have similar means, reduced or more extensive compared to the State concerned.

As outlined above, Adrian Miroiu argues that the rational individual is endowed with three attributes, namely perfect rationality, action to satisfy one's own interest, and possession of perfect information. According to perfect rationality, the state, in order to ensure cyber security, has the ability to choose between alternatives (various policies, attack or defense, retaliation, extended or limited response, etc.), to make comparisons between the options at hand according to the means it has and to operate with a hierarchy of interests, All in the idea of choosing the best alternative.

Aiming at action in its own interest, the state, in the actions it takes to ensure cyber security, pursues its own objective, namely security, but does not seek from the start to help other states, nor to cause them damage without any well-founded reason.

Finally, the state should be an individual entity that has perfect information, but this is an ideal desideratum, because we have shown above that it is difficult for it to have all the necessary information. Thus, the state will make the decision in the field of ensuring cyber security having at hand all the information available at any given time.

Finally, the state, as a rational entity, can also act according to the Rawlsian principle of maximin. According to the maximin principle, the state will not aim to take risks in ensuring cybersecurity. In a given situation, especially of risk or threat, the state will tend to choose the least possible evil, not necessarily the best outcome, this strategy being suitable for a decision-making situation in conditions of uncertainty.

## 4. Conclusions

This paper considered the issue of state action to ensure security in cyberspace, from the perspective of rational choice theory. Rational choice theory, as an approach, can be a good analytical perspective in the field of state action in cybersecurity management. The paper started from the assumption that the state, seen as a unitary, individual entity, represents a rational actor, with its own interests, which it hierarchizes, and with objectives that it defines according to the means at its disposal.

Even if, traditionally, the state, as the depository of the legitimate monople on coercion in the Weberian sense, reserves as its manager the domains of security in land, air and sea space, it is also reserved for the management of cyberspace by means of specific means.

Apart from the military domain, the scope of cybersecurity can extend to objectives such as critical infrastructures (energy, transport, healthcare), private banking or any other entities, large or small, private or state-owned. Military objectives should not be ignored, whether is military bases, offensive or defensive equipment, or sensitive databases.

**References:**

1. Buchanan, J. M. and Tullock, G., 1962. *The Calculus of Consent: Logical Foundations of Constitutional Democracy*. Ann Arbor Paperbacks: University of Michigan Press.
2. Georgescu-Roegen, N., 1974. *The Entropy Law and the Economic Process.* Cambridge, Massachusetts: Cambridge University Press.
3. Grünberg, L., 1989. Knowledge and values. The problem of axiological rationality, in Ludwig G. ed. *Human ontology*. Bucharest: Romanaian Academy Publishing House.
4. Kianpour, M., Kowalski, S. J. and Overby H., 2021. Systemically understanding cybersecurity economics: a survey. *Sustainability*, 13(24), 13677, pp.1-28.
5. Mearsheimer, J.J. and Rosato, S., 2023. *How States Think. The Rationality of Foreign Policy.* New Heaven and London: Yale University Press.
6. Mearsheimer, J.J., 2003. The tragedy of force politics. *Offensive realism and power struggle*. [translation into Romanian]. Header XX Press.
7. Mill, J.S., 1863. *Utilitarianism and On Liberty Including Mill's 'Essay on Bentham' and selections from the writings of Jeremy Bentham and John Austin*. Reprint 2003. Blackwell Publishing.
8. Miroiu, A., 2006. *Fundamentals of Politics, vol. 1 : Preferences and collective choices* [in Romanian: *Fundamentele politicii. Vol I. Preferințe și alegeri colective*]. Iasi: Polirom.
9. NATO, 2023. *Cyber defence*. [online] Available at: <https://www.nato.int/cps/en/natohq/topics_78170.htm> [Accessed 1 May 2024].
10. Nurmi, H., 1983. Voting Procedures: A Summary Analysis. *British Journal of Political Science*, 13(2), pp.181-208
11. Rawls, J., 1971. *A Theory of Justice*. Cambridge: The Belknap Press of Harvard University Press.
12. Sargent, T. and Wallace, N., 1974. *Rational Expectations and the Theory of Economic Policy*. University of Minnesota.
13. Sen, A. K.. 1987. *On Ethics and Economics*. Oxford: Blackwell.

14. Simon, H. A., 1983. *Reason in Human Affairs.* Stanford, California: Stanford Univeristy Press.
15. Sims, C. A., Stephen M. G. and Jeffrey D. S., 1982. Policy Analysis with Econometric Models. *Brookings Papers on Economic Activity.* 1, pp. 107–164. [online] Available at: <https://doi.org/10.2307/2534318> [Accessed 1 May 2024].
16. Ungureanu, M., 2018. Expected utility and rationality in neoclassical economics. In: Ungureanu, M. ed. 2018. *Economics and Decision Psychology Introduction to Behavioral Economics.* Iasi: European Institute, pp.19-62.
17. Von Solms, R. and van Niekerk, J., 2013. From information security to cyber security. *Computers and Security,* 38, pp.97-102.
18. Weber, M., 1968. *Economy and Society,* vol. 1. In: G. Roth, G. and Wittich, C. ed. 1968. Berkeley: University of California Press.