**Saint-Petersburg State University**

**Department of International Relations**

**CRITICAL THEORY OF INTERNATIONAL RELATIONS AND GLOBAL CYBERSECURITY**

**отображается**

**Prepared by**

**The 2nd grade Master’s student**

**Askhad Shidukov**

**Introduction**

The purpose of this chapter is rather straightforward. It is very unusual, almost unique insofar as critical theory is still marginal within the field of International Relations, however, it already challenged traditional theories of International Relations. Thus, this needs to be explained. In this chapter, we will recount, summarize, and emphasize on basic assumptions of Critical Theory of International Relations, analyze its background, and attempt to apply some of the basic ideas of critical theory to global cybersecurity. We do this in basically three steps. We begin with the discussion of critical theory’s background and the necessity for a structural rethinking of security in International Relations. We then overview the basic ideas of critical theory of international relations and analyze the works of the biggest representatives of this theory. After that, we link security critical theory to global cybersecurity and appraise the utility of critical theory in International cyber politics. While traditional theoretical models of International Relations, such as Realism, can be rather helpful when analyzing the international relations dimension of NATO-EU cooperation, they frequently lack a critical engagement. This Master Dissertation implies Critical Security Studies (CSS) to analyze cyberspace and the impact it has on the relations between the European Union and NATO.

Even though we make a comparison of critical theory with traditional theories, we do not claim to present a detailed comparison of critical theory to traditional International Relations theories.

To achieve the aforementioned goals, we use qualitative methods of research in International Relations. We use comparative research. A structurationist approach is also used in this thesis.

**I. Critical theory of International Relations**

**1.1 Background of the Critical theory of International Relations**

The need for a structural rethinking of security in International Relations was demonstrated by political, social, and economic circumstances which occurred as soon as the Soviet Union collapsed, and the Cold War was brought to its end. Traditional schools of thought of International Relations were state-centristic and mostly neglected transnational, supranational, and subnational factors and their role in International Relations. For example, major upheavals in International Relations such as the demise of the USSR and September 11 Terrorist attacks represent a crucial milestone and a turning point in the development of International Relations theory inasmuch as they demonstrated to the scholars and researches that state-centristic theories of IR were no longer able to take into consideration new emerging issues and thus traditional theories were no longer of practical validity. No traditional theory was able to go beyond the framework of analyzing state-system interaction and concentrate on the events within the state. This is one of the major reasons why traditional theories were unable to foresee the demise of the Soviet Union. The rise of nationalism in Eastern Europe, the collapse of the confidence in Marxism-Leninism and in communism in general, the rise of influence over the Soviet leaders by alternative security thinking, and other big factors were not taken into account by traditional theories because it went outside of the traditional paradigm. In this regard, the representatives of the Welsh School of International Relations, Richard Wyn Jones and Ken Booth proposed a new approach to security policy, which was influenced by the Frankfurt school and Gramscian's thinking. Not only had they proposed a new analytical perspective that could meet the need for decentralizing the state as a reference object of research, critical theory has proven to be a valuable tool in the service of security research to meet the growing need for a broader research framework which helped overcome the theoretical axiom that in the second half of the 20th century turned security thinking into a simple dichotomous competition.

Founded by the Frankfurt School, a group of German intellectuals associated with the Institute of Social Research at the University of Frankfurt in the 1920s-1960s (including Max Horkheimer, Theodor W. Adorno, Herbert Marcuse, and Walter Benjamin), critical theory was applied to international relations by Robert Cox in the early 1980s, and that is why R. Cox may be regarded as the father of critical theory of International Relations. But that notwithstanding some respected researches in the field of International Relations propose to divide the scholars of this theory into two large generations: ‘the first generation’ which includes German social theorists and philosophers such as Herbert Marcuse, Max Horkheimer, and Theodor W. Adorno, and ‘the second generation’ which include such philosophical schools of thought in the field of International Relations as neo-Marxism, Social constructivism, Critical Theory, feminism, neo-Gramscianism, and the others. Sensu stricto, both generations of these schools of thought of International Relations try to change the entirely descriptive type of social science to an exploratory one. Critical theory’s analytical purpose and theoretical assumptions make it different from traditional IR theories. Its ideas originate from Freudian, Marxist as well as Kantian culture and primarily focuses on the idea of human emancipation from the modern state and economic system, social practices, and repressive institutions, by supporting ideas that meet universalist principles of justice.

**1.2 The Basics of Critical Theory**

As I have already stated above, even though critical theory embraces a big number of different assumptions and approaches, the concept of ‘emancipation’ of Kantian and Marxist traditions are at the base of critical theory’s lineage. Kant and Marx, with their universal aspirations, become central figures for critical theory in modern times insofar as they both proposed revolutionary ideas about new ways to reshape the world. Immanuel Kant contributed to the development of the cosmopolitan and supranational political communities by his claims of the increasing interconnectedness of the world. It has to be noted that Kant initiated an approach to IR theory that went beyond the traditional framework of thinking of world politics as simply interstate politics. He anticipated modern theories of International Relations which are taking into account international terrorism, world economy, environmental issues, arms control, and social movements as central objectives of concern in the determination of domestic policy.

On the other hand, Karl Marx, historian, economist and socialist who wrote the works that formed the basis of communism. Marx’s works largely contributed to the development of the critical theory of International Relations. His critique of a capitalist economic system says that we, as participants of capitalist economic relations, understand the economy in terms of free exchange, private property rights and the rule of demand and supply, and in doing so, we start thinking about the capitalist economic system as justified and how it should be whereas this way of thinking is nothing more than an ideology. An ideology that obscures from its participants destructive labor exploitation and the creation of an unfair economic system. Marx’s critical theory of the economic system was later on developed by the representatives of the Frankfurt School of IR and especially by Adorno, Marcuse, Habermas, and Horkheimer.

Having analyzed the very base of critical theory’s lineage, we noticed that Marx and Kant focused on different research areas and postulation, but that notwithstanding there is a common defining feature of critical theory which is the need for systematic change for human emancipation and global freedom. The aforementioned need for systematic change for human emancipation and global freedom does not represent the majority of critical theory’s assumptions nor it helps to understand the contemporary sense of critical theory, and that is why recent sources of critical theory are to be further analyzed: Antonio Gramsci and his influence over Robert Cox, Jürgen Habermas, Andrew Linklater.

Antonio Gramsci is one of the most influential thinkers of the 20th century. Gramsci’s theory of hegemony proposed a new complex nature of the state, by introducing the “relationship between the dominant and dominated classes”. Hegemony, according to Antonio Gramsci, is the use of moral, intellectual, economic, political, and other forms of power by the dominant class to achieve its goals and to do so, this dominant class is to establish its worldview as universally accepted by the people. In this regard, the state is not a unipolar actor in the international arena, as it is comprehended by the realists. Moreover, Gramscianism, instead of accepting the realistic understanding of the anarchical system approach, believes that states become bound together on the international arena insofar as they accept bourgeoisie morals as well as values[[1]](#footnote-1).

The second distinction to be made between the realist approach and Gramsci’s theory is their understanding of Security dilemma. According to John H. Herz, states, concerned about their security from being attacked or dominated, strive to attain security[[2]](#footnote-2). Thus, states are trying to acquire more power to secure themselves. But these actions, on the contrary, rendering them more insecure inasmuch as the others start preparing for the worst and accumulate more power. Some scholars of international relations have claimed that security dilemma is the most crucial source of conflict. We can then, following John Herz’s work, explain the vicious circle of arm race between the Soviet Union and the United States of America which was on presumably since 1945 up to the end of the demise of the USSR in 1991, since both superpowers sought primarily to secure themselves by the accumulation of nuclear weapons. Gramscian theory of hegemony sees differently Security dilemma. As it was mentioned above, Gramsci’s theory of hegemony understanding lies within class-relation and relations between dominant and dominated. A coercive force is considered to be the primary instrument of the dominant-class inasmuch as it has the ability to keep dominated groups disorganized and convinced that moral principles that were established are universally accepted. In this regard, the main reason for the collapse of the Soviet Union may be found in the dissemination within the soviet civil society of bourgeoisie ideology, morals, and values.

The next prominent scholar who largely contributed to the development of critical theory is Robert Cox that was influenced by Antonio Gramsci. Robert Cox, according to some scholars, may be regarded as the father of critical theory[[3]](#footnote-3). According to Robert Cox, critical theory differs dramatically from traditional theories insofar as it is anti-status-quoist since it «allows for a normative choice in favor of a social and political order different from the prevailing order”[[4]](#footnote-4). His famous formula – “a theory is always for someone and for some purpose” recalls that all theories have a perspective, which itself "derives from a position in time and space, especially social and political"[[5]](#footnote-5).

Robert Cox presents critical theory as opposed to problem-solving theory, corresponding to what Horkheimer called "traditional theory", which "takes the world as it finds it". Dominant theories such as the neorealism of Waltz or the Liberal neo-institutionalism of Keohane are, for Cox, typical cases of problem-solving theories. Critical theory, on the contrary, "wonders how this order was born. [It] does not take institutions and social and power relations for granted, but challenges them." This theory is "critical" in that it challenges the dominant order, questions "where it comes from" and it is also normative in that it is based on "a normative choice in favor of a social and political order different from the dominant order, but it limits the range of choices to the alternative orders that constitute achievable transformations of the existing world". It is thus, unlike problem-solving theory, historical not just because it analyzes the past, but it is concerned with a continuing process of historical change since social, economic, or political orders are not fixed in space and time. Because critical theory of International Relations deals with a continuing process of historical change, it is more adjusted to grips with the changing reality to better comprehend the world it has to deal with, understand, and explain rather than problem-solving theory.

The other major distinction to be made here between critical theory and problem-solving theory is the understanding of the possibilities of state’ changes. Problem-solving theory does not call into question states in terms of the possibilities of fundamental changes since they occur within a limited framework, whereas critical theory goes beyond it and it searches for its origins and the developmental possibilities of fundamental change.

Cox took the Gramsci's theory of hegemony and applied it to the World order, rather than to International relations inasmuch as the latter is a very state-centristic term. Rather than mere domination, hegemony is a subtle balance between coercion and consent: dominated states do not suffer their subordination as a constraint, on the contrary, it seems to them natural, therefore acceptable, and they even participate in it because they feel that it is in their interest. In this sense, hegemony is «the recruitment of other people in the exercise of your power by convincing them, cajoling them, and forcing them to believe that they want what you want." It is not just inter-state but is expressed "in universal norms, institutions, and mechanisms which lay down general rules of behavior for states and for those forces of civil society that act across national boundaries – rules which support the dominant mode of production"[[6]](#footnote-6). For example, Cox explains, the periods 1845-1875 and 1945-1965 were hegemonic, around the United Kingdom and the United States respectively.

As was aforementioned, Robert Cox analyzed world order, rather than International Relations. In doing so, he challenges the state-centristic realism’s study of interstate relations which does not take into consideration social forces. This is, according to Cox, a misleading way of analyzing International Relations. Instead of focusing on interstate relations, Robert Cox proposes to focus on the state form and how it can be changed under the influence of civil society and other macro forces. Productive forces, ideas, and institutions are crucial in the analysis of ‘world order’ or ‘global politics’ or ‘global political economy’[[7]](#footnote-7).

Having analyzed literature on critical theory of International Relations, we can distinguish major assumptions of critical theory of IR:

1. States are not the only actors of World Politics According to Robert Cox, social constructs are the principal actors of World Politics;
2. The major purpose of theory is to provide understanding and practical knowledge for further emancipation. Theory should be able to be altered to grips with the changing reality for better understanding of the world it deals with;
3. States and the system in which they operate are not unchangeable since they are not fixed in time and space;
4. The appropriate methodology is that which focus is on relations between social structures and states.

**II. Critical Theory’s vision of Cybersecurity**

**2.1 Critical theory and Security Studies**

The Aberystwyth School (sometimes The Welsh School) of security studies or Critical Security Studies (CSS) is based on the works of Richard Wyn Jones and Ken Booth. It has to be noted that both of them were influenced by Gramsci’s theory and Frankfurt School. As all of them have their roots in Marxism, they are all oriented towards the elaboration of a theory that would be aimed at the systemic transformation for human emancipation and the creation of a free global community. Emancipation, according to critical theory, implies liberty but of an egalitarian character. It requires the integration of reciprocal rights[[8]](#footnote-8).

Critical security studies are opposed to the traditional security studies which have dominated the subject for half a century. Traditional security thinking is rather status quo oriented and it is of state-centristic nature. For Richard Wyn Jones and Ken Booth traditional approaches, such as the realistic approach, can never lead to true security as they focus on ‘power’ and ‘order’ and emphasize the need of strong states and military power. Traditional theories focus more on military force, not on security itself. Ken Booth considers realism to be an ‘unrealistic’ ideology that is too narrow, and its assumptions go against human interests. Moreover, this realistic ‘ideology’, pretending to be a theory of knowledge, largely lacks methodology[[9]](#footnote-9).

Unlike traditional theories which consider states as the central security actor and the principal security provider, CSS claims that states are the ones that render humankind insecure since way more people were killed by their own governments rather than by foreign armies or foreign governments. Security, according to Booth, can be achieved only when it is understood as emancipation. ‘Emancipation’ and ‘security’ are of the same meaning in CSS. In order to achieve it, we are to conceptualize the term ‘security’ and understand why people and groups feel insecure and suffer from it. Apparently, Ken Booth claims, biological motivations for security are universal, that is the necessity to have shelter, food, to feel secure physically, etc. Thus, the core elements of ‘security’ are universal biological motivations. In order to achieve global security, people should create security communities, made up of free communities and cosmopolitan states. Global governance which is composed of emancipated governments will be able to transcend the Security dilemma, which is the most crucial source of conflict. Emancipation, not power or order, produces true security, inasmuch as it enables people to go beyond barriers between ‘us’ and ‘them’. In perusing emancipation, real security can be attained[[10]](#footnote-10).

Therefore, having analyzed the Critical Security Studies, we may conclude that there are three core ideas that underpin CSS. The first core idea is that security is a derivative concept; that is, security reflects deeper assumptions about the nature of politics and the role of conflict in political life. It connotes that human’s understanding of security comes from the way one’s thinks about the world and the politics. The ideas intentionally disseminated in the human’s society by specific actors will always influence the way we think, perceive, and understand threats. It ultimately influences the way we define security itself.

The second idea of CSS consists of the argument that the security agenda must be broadened. Military force, according to Barry Buzan, should not be considered as the only potential threat. Five different sectors such as the environment, the economic, the political, the military and the societal should also be analyzed. “Military security concerns the two-level interplay of the armed offensive and defensive capabilities of states, and states' perceptions of each other's intentions. Political security concerns the organizational stability of states, systems of government, and the ideologies that give them legitimacy. Economic security concerns access to the resources, finance and markets necessary to sustain acceptable levels of welfare and state power. Societal security concerns the ability of societies to reproduce their traditional patterns of language, culture, association, and religious and national identity and custom within acceptable conditions for evolution. Environmental security concerns the maintenance of the local and the planetary biosphere as the essential support system on which all other human enterprises depend. These five sectors do not operate in isolation from each other. Each defines a focal point within the security problematique, and a way of ordering priorities, but all are woven together in a strong web of linkage”[[11]](#footnote-11)

**(NOT FINISHED)**

**2.2 CSS and Cybersecurity**

**(DRAFT)**

With the proliferation of Information and Communication Technologies (ICTs), Internet has become one of the greatest equalizers. Interest in cybersecurity has never been greater among International Relations scholars. Nowadays the Internet provides us with the possibility to communicate with one another across the globe. It also provides with a medium for ideological, cultural, and informational exchange. Such previously unimaginable level of interconnectedness benefits not only civilians, but also businesses and governments. But that notwithstanding, for all goods, the widespread of the Internet represents series of great threats. From the financial loss of businesses through cyber threats, the leak of classified government data happed due to cyber-attacks may pose huge challenge to national and economic security of nations. The cyber and hybrid threats are increasingly seen as a strategic challenge.

It must be stated that cyberattacks have become way more disruptive, expensive, and political. Cyberattacks by foreign states or non-state actors against critical infrastructure, democratic institutions, academic, military, economic systems of both NATO and the European Union Member States have significantly multiplied. Nowadays the humankind lives in information society where sensitive government databases may be invaded by foreign governments; criminals attacking servers and databases form their bedrooms or ever bored computer-literate teenagers.

**References:**

1. Booth, K. (1991). Security and Emancipation. Review of International Studies, 17(4).
2. Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. International Affairs (Royal Institute of International Affairs 1944-), 67(3), 431–451. JSTOR. https://doi.org/10.2307/2621945.
3. Christopher Grundy, What is the Difference Between a Realist and a Gramscian Understanding of Hegemony? [Electronic resource]. – International Relations. URL: https://www.e-ir.info/2012/06/08/what-is-the-difference-between-a-realist-and-a-gramscian-understanding-of-hegemony/.
4. Cox, R.W. (1981). Social Forces, States and World Orders: Beyond International Relations Theory. Millennium: Journal of International Studies 10(2).
5. Cox, Robert W. “Gramsci, Hegemony and International Relations : An Essay in Method.” Millennium 12, no. 2 (June 1983): 162–75. https://doi.org/10.1177/03058298830120020701.
6. Herz, John H. "Idealist Internationalism and the Security Dilemma." World Politics 2, no. 2 (1950): 157-80. Accessed October 25, 2021. doi:10.2307/2009187.
7. Krause, Keith. "Critical Theory And Security Studies: The Research Programme of 'Critical Security Studies'." Cooperation and Conflict 33, no. 3 (1998): 298-333. Accessed October 24, 2021. http://www.jstor.org/stable/45083929.
8. Leysens A. (2008) The Legacy of Coxian Critical Theory. In: The Critical Theory of Robert W. Cox. International Political Economy Series. Palgrave Macmillan, London. https://doi.org/10.1057/9780230584457\_6.
9. Marcos Farias Ferreira, Introducing Critical Theory in International Relations [Electronic resource]. – International Relations. URL: https://www.e-ir.info/2018/02/18/introducing-critical-theory-in-international-relations/.
10. Matt Davies, IR Theory: Problem-Solving Theory Versus Critical Theory? [Electronic resource]. – International Relations. URL: https://www.e-ir.info/2014/09/19/ir-theory-problem-solving-theory-versus-critical-theory/.
11. Moolakkattu JS. Robert W. Cox and Critical Theory of International Relations. International Studies. 2009;46(4):439-456. doi:10.1177/002088171004600404.
12. Nunes, João. "Reclaiming the Political: Emancipation and Critique in Security Studies." Security Dialogue 43, no. 4 (2012): 345-61. Accessed October 25, 2021. http://www.jstor.org/stable/26301921.
13. Sallach, David L. "Class Domination and Ideological Hegemony." The Sociological Quarterly 15, no. 1 (1974): 38-50. Accessed October 25, 2021. http://www.jstor.org/stable/4105619.
14. Wyn Jones, R. (1999). Security, strategy and critical theory. Colorado: Lynne Rienner Publications.
15. Zaslavskaya N. (2017). ‘Theories of International Relations’, in Russia and the World. (ed.). Lexington Books: Maryland. pp. 35-37.

Dépourvue d’une quelconque définition légale, ou d’un consensus de la doctrine, la notion de « cyber-arme » est difficile à définir. Ayant émergé dans le langage commun en 2010 avec l’affaire Stuxnet2 , elle demeure marginale dans la réflexion sur les cyberconflits.

Cette difficulté est accrue si on considère que la littérature scientifique se réfère au cyberespace en tant qu’arme. Les auteurs ont par ailleurs tendance à distinguer entre cyberattaque et cyberdéfense3 . Par analogie, il est alors possible d’associer alors l’attaque à la notion d’arme. Mais c’est bien dans la littérature anglo-saxonne que la notion de cyber-arme est le plus souvent employée. Les «  cyberweapons  » y sont alors présentées comme, des outils informatiques de nature diverse opposés aux classiques malwares. Même présentes et identifiées, les analyses sur ces objets restent relativement rares.

Une fois ces problèmes de définition dépassés, le principe de l’existence d’un marché spécifique des cyberarmes et de sa dynamique apparaît d’autant plus problématique. Les développements suivants reprendront dès lors les hypothèses développées par Thomas Rid et par Peter McBurney4 . Leur approche offre un cadre général et elle permet de traiter l’ensemble des logiciels malveillants sans établir de distinction artificielle entre la cyber-arme et le malware. L’enjeu de cette question n’est pas où acheter un virus informatique, mais bel et bien de savoir si ce type de logiciel dispose de caractéristiques facilitant la construction d’un cadre d’échange propice à sa prolifération en tant que cyber-arme.

D’autre part, derrière l’idée d’un marché des cyber-armes surgit l’idée de la prolifération de celles-ci. Or la définition proposée par ces deux auteurs s’avère assez restrictive. Elle conduit à conclure que le nombre des cyber-armes telles que Stuxnet auront vocation de par leurs coûts de développement et de mise en œuvre à demeurer des exceptions plutôt qu’une tendance. Ce constat tend à questionner finalement l’avenir d’un marché dédié aux cyber-armes. En outre, la confrontation de cette définition avec le concept de marché, replacé dans le contexte général du cyberconflit, viendra dévoiler un certain nombre d’interrogations et de faiblesses de la notion même de cyber-arme. De nos jours, le « marché cyber » peut tout être, sauf un marché de la cyber-arme.

La cyber-arme : de quoi s’agit-il ?

L’expression cyber-arme peut recouvrir deux logiques complémentaires : D’une part, elle peut permettre d’envisager l’outil technique et le moyen déterminant le caractère cybernétique d’une attaque. D’autre part, elle aurait vocation à englober l’ensemble des moyens techniques, matériels et humains dédiés aux cyber-attaques. C’est ainsi que la cyberarme incarne au choix un ensemble détaillé de logiciels précis, ou le champ cyber dans son ensemble. Dans le premier cas, adopter le point de vue de la cyber-arme revient à restreindre très fortement l’analyse. Dans le second cas, la notion de cyber-arme n’a tout simplement plus aucun intérêt.

Réfutant la notion de cyber-guerre qu’ils jugent inappropriée, Thomas Rid et Peter McBurney défendent l’idée d’une cyber-arme qui dépasse la seule composante cyber d’un conflit. Ce choix les conduit à la première solution , et à une conception très restrictive : le « weaponised software ». Si une arme désigne tout outil conçu pour menacer ou pour causer des dommages physiques, fonctionnels ou psychologiques à des structures, des systèmes ou des êtres vivants, alors la cyber-arme est simplement le code informatique utilisé pour des objectifs identiques5 .

Le niveau technique et donc le niveau de puissance de ces «  cyberarmes » fournit alors un critère pour une première typologie : ➤ les armes dites à faible potentiel, génériques, peu discrètes et d’acquisition facile, faciles à mettre en place et à contrer6  ; ➤ les armes à fort potentiel, spécifiques, nécessitant des investissements lourds7  ; ➤ les armes combinant des caractéristiques de ces deux catégories8 .

Dans la conception de ces armes, l’accroissement du potentiel destructeur induit deux efforts : d’une part, au niveau des ressources (Temps/ Recherche/Investissement) ; d’autre part, au niveau du ciblage. Ces efforts participent à la réduction du nombre des dommages collatéraux potentiels de l’arme, réduisant également son pouvoir de coercition et de menace. Tout en sachant qu’une cyber-arme dispose d’une durée limitée pour agir avant que les défenses n’évoluent suffisamment pour la contrer.

L’exploitation des bugs et l’espionnage par l’intermédiaires des chevaux de Troie ne sont pas regardées comme des cyber-armes car moins dangereux9  ; ils appelleraient des sanctions juridiques différentes. Le coût prohibitif des cyber-armes à fort potentiel entraîne la diminution de leur risque de prolifération, comme n’importe quel autre système d’arme. De plus en raison du degré de précision (penser pour une cible identifiée voire unique), la cyber-arme dans son acception la plus restrictive devient difficilement « exportable ». De manière connexe, ceci tend à remettre en cause le postulat de la prééminence de l’attaque sur la défense dans le champ cyber. La défense est davantage présentée sous un jour favorable en raison de son coût moindre, donc de sa plus grande vitesse d’évolution.

Construite notamment sur le constat d’une absence de définition dans la doctrine américaine10, cette approche s’avère intéressante pour différentes raisons.

Premièrement, face à une définition politisée et discutée de ce qu’est et de ce que doit être le cyberespace, il faut ici saluer l’effort qui consiste à vouloir réintégrer une forme de granularité technologique dans le raisonnement. Si on doit garder une vision normative de la définition proposée ici, il faut cependant considérer que cette granularité se construit en opposition avec l’idée de neutralité technologique qui conditionne la viabilité et la durabilité d’une norme par rapport aux évolutions de l’état de la technique. Si la notion de cyber-arme reste assez floue pour permettre une certaine interopérabilité dans la désignation, il faut mettre en avant sa spécificité.

Deuxièmement, en voulant s’affranchir de la cyber-guerre, Thomas Rid et Peter McBurney excluent de leur paradigme la question de l’acteur. On retrouve bien l’intention de nuire et la perception de la menace comme conditions de l’action ou encore l’effet psychologique sur la cible. Toutefois, ce sont ici des considérations qui semblent secondaires pour les auteurs. La question de la cyber-arme ne se pose pas en vertu de l’identité ou de la nature des acteurs. Corolairement, la cyber-arme n’est donc pas obligatoirement régalienne.

Enfin, on assiste à un paradoxe : d’un côté ce renoncement à l’acteur s’inscrit théoriquement dans les conceptions stratégiques qui font de la multiplication du nombre d’attaques un produit de la densification et de la complexification des réseaux. De l’autre côté, le recours à une cyber-arme ne peut s’inscrire que dans un intérêt bien précis. Il s’agit de l’idée d’une émergence de cyber-attaques raisonnées et pensées comme une réalité dont les objectifs peuvent être économiques, idéologiques et/ ou militaires. Les intérêts conditionnent ainsi paradoxalement la cyberarme indépendamment (semble-t-il) de leurs propriétaires réduits à des propensions marginales.

Ainsi, adopter une approche restrictive de la cyber-arme conduit à décrire un ensemble précis et déterminé de logiciels malveillants. Cependant, cet ensemble qui n’est pas neutre est incapable de traduire la cyberattaque dans toute sa complexité et dans sa variété, et ignore les questions de l’exploitation des failles, du mécanisme de défense et des acteurs. De fait, la cyber-arme est un point de vue inefficace qui conduira à exclure la prise en compte de l’intégralité des marchés les plus fleurissants du secteur, notamment le marché global des technologies de sécurité informatique ou encore le marché des failles et de leurs codes d’exploitation.

Un marché des cyber-armes au prix de nombreuses exclusions.

Cet effort de définition est parmi les plus aboutis en ce qui concerne la cyber-arme. Toutefois, il ne peut être regardé comme suffisant pour répondre à la question de savoir s’il existe un marché des cyber-armes. Plus encore, il s’avère un obstacle à cette démarche. Car si le marché se conçoit comme un cadre de rencontre entre l’offre et la demande, plusieurs interrogations demeurent en suspens quand à l’intérêt et à l’organisation d’une telle structure pour les cyber-armes ainsi désignées. La grande question que l’on peut se poser est celle du secteur à considérer et de ses subdivisions (à inclure ou à exclure). Enfin, le caractère transparent de l’acteur dans la définition de la cyber-arme ne permettra pas de trancher la question du statut légal par essence de ce type de marché. Indépendamment de la confidentialité intuitive autour de ces échanges, il est impossible de savoir si nous avons à faire à un marché gris ou noir, sans se plonger dans la question de l’acteur qui devra faire l’objet de développements à part...

Pris dans l’idée d’une arme à faible potentiel, le marché est déjà existant depuis 1986/87 puisqu’il s’agit du marché des virus (et des antivirus) ; lequel est connu de tous et facilement accessible, y compris pour n’importe quel particulier. Notre idée du marché des cyber-armes passerait donc écessairement par le marché du virus informatique à l’exclusion des chevaux de Troie, des spywares ainsi que des virus « zombificateurs » qui sont hors de la définition. Il faut également exclure les équipements et les logiciels destinées à la protection des systèmes d’information ; nous touchons ici également, une des limites de cette définition de la cyber-arme ; elle ne prend pas en compte les moyens de se prémunir des attaques11.

Il nous faut exclure également les logiciels de chiffrement ainsi que des outils qui permettent de se dissimuler, au-delà du marché des logiciels viraux et des technologies de sécurité entendues globalement. Comme le bug n’est pas regardé comme une cyber-arme, un autre domaine est à exclure malgré son caractère lucratif : le marché des vulnérabilités et de leurs codes d’exploitation12. Des failles, comme par exemple Heartbleed, ne pourraient être incluses dans le marché de la cyber-arme. La réponse à cette première interrogation tient donc dans l’idée que si l’arme à faible potentiel peut s’inscrire dans le marché des technologies de sécurité, elle ne peut caractériser l’essence d’un marché spécifique des cyber-armes à elle seule à cause des nombreuses exclusions opérées. Par ailleurs, la question initiale perd ainsi totalement de son intérêt. Le phénomène cyber ne serait porteur d’aucune originalité.

Pour répondre à cette question de l’existence d’un marché des cyberarmes de manière utile, il faudrait que la définition permette de dégager un nouveau marché uniquement dédié aux armes à fort potentiel. Et si un marché des cyber-armes existe avec toutes les restrictions évoquées, d’autres interrogations émergent notamment sur l’objet et sur le moment de l’échange. L’échange entre les acteurs de ce marché intervient-il au moment de la création de la cyber-arme ou de sa mise en œuvre ? Autrement dit, le marché de la cyber-arme est-il un marché de services ou un marché de biens ? Dans le premier cas, l’acheteur cherche des compétences afin de bâtir une cyber-arme qui serve ses objectifs tandis que le vendeur dispose de ces compétences. Dans le second cas, l’acheteur recherche une solution « clefen-main » tandis que le vendeur propose des cyber-armes prêtes à l’emploi. Ce second cas correspondrait davantage au logiques d’une arme à faible potentiel. Autrement-dit, compte-tenu des contraintes d’élaboration de l’arme, l’hypothèse d’un marché uniquement dédié aux cyber-armes à fort potentiel ne peut être qu’un cadre d’échange pour les compétences utiles ou/et des services entre un vendeur dépositaire de savoir-faire et un acheteur animé par un intérêt extrêmement précis (au sens qu’il ne peut trouver satisfaction sur les autres marchés du secteur). Le marché du travail existe bel et bien dans le champ cyber, seulement ce n’est pas un marché spécifiquement dédié à la conception de cyber-armes à haut potentiel...

Le marché de la cyber-arme ne peut ainsi exister sans englober le marché cyber dans son ensemble. Le risque de prolifération de la cyber-arme est limité par les importantes contraintes qu’elle impose à son utilisateur en matière de conception et d’emploi. En l’effet, les cyber-armes à faible potentiel disposent de marchés déjà connus. La question de l’existence d’un marché de cyber-arme trouve alors un intérêt inexistant. L’hypothèse d’un marché des cyber-armes à haut potentiel fondé sur l’échange de savoir faire destiné à la construction de ces mêmes armes ne peut se réaliser qu’au travers d’un ensemble plus vaste qui n’est pas spécifique en incluant des produits, et des services qui ne peuvent être regardés comme des cyberarmes.

Ainsi, bien qu’elle ne soit pas sans intérêt, la notion de cyber-arme ne peut servir à justifier de l’existence d’un seul et unique marché dédié. La prise en compte de la définition de la cyber-arme, ainsi que des exclusions auxquelles elle conduit, amène par ailleurs à replacer le risque par rapport aux autres risques du secteur. Car, il existe enfin plusieurs marchés sur lesquels ne s’échangent pas de cyber-armes mais des produits qui peuvent s’avérer tout aussi dangereux, voire causer bien plus de dommages (vulnérabilités, trojans...). Cette question conduit donc à nuancer le caractère terrifiant d’une cyber-arme à haut potentiel.

Au-delà de la question du marché, penser la question du risque au travers de la notion de cyber-arme est de nature à induire une erreur dans l’évaluation de ce dernier. Cette hypothèse pose tout simplement la question de l’utilité de cette notion. Une défense efficace ne peut se concevoir sous l’angle de la cyber-arme

1. Sallach, David L. "Class Domination and Ideological Hegemony." The Sociological Quarterly 15, no. 1 (1974): 38-50. Accessed December 8, 2020. http://www.jstor.org/stable/4105619. [↑](#footnote-ref-1)
2. Herz, John H. "Idealist Internationalism and the Security Dilemma." World Politics 2, no. 2 (1950): 157-80. Accessed December 7, 2020. doi:10.2307/2009187. [↑](#footnote-ref-2)
3. Zaslavskaya N. (2017). ‘Theories of International Relations’, in Russia and the World. (ed.). Lexington Books: Maryland. pp. 35-37. [↑](#footnote-ref-3)
4. Cox, Robert W. “Social Forces, States and World Orders: Beyond International Relations Theory.” Millennium 10, no. 2 (June 1981): 126–55. https://doi.org/10.1177/03058298810100020501. [↑](#footnote-ref-4)
5. Ibid. [↑](#footnote-ref-5)
6. Cox, Robert W. “Gramsci, Hegemony and International Relations: An Essay in Method.” Millennium 12, no. 2 (June 1983): 162–75. https://doi.org/10.1177/03058298830120020701. [↑](#footnote-ref-6)
7. Cox, Robert W. “Gramsci, Hegemony and International Relations: An Essay in Method.” Millennium 12, no. 2 (June 1983): 162–75. https://doi.org/10.1177/03058298830120020701. [↑](#footnote-ref-7)
8. Krause, Keith. "Critical Theory And Security Studies: The Research Programme of 'Critical Security Studies'." Cooperation and Conflict 33, no. 3 (1998): 298-333. Accessed December 7, 2020. http://www.jstor.org/stable/45083929. [↑](#footnote-ref-8)
9. Wyn Jones, R. (1999). Security, strategy and critical theory. Colorado: Lynne Rienner Publications. [↑](#footnote-ref-9)
10. Booth, Ken. (1991). “Security and Emancipation”, Review of International Studies, Vol. 17, No. 4 (Oct., 1991), pp. 313-326. [↑](#footnote-ref-10)
11. Buzan, B. (1991). New Patterns of Global Security in the Twenty-First Century. International Affairs (Royal Institute of International Affairs 1944-), 67(3), 431–451. JSTOR. https://doi.org/10.2307/2621945 [↑](#footnote-ref-11)