ASSET FUNGIBILITY AND ORGANIZATIONAL ADAPTABILITY: THE EU AND NATO’S APPROACHES TO MANAGING AND REGULATING CYBER THREATS

Abstract:

In the last decade the NATO and the European Union (EU) have paid close attention and have stressed the importance of cyber threats in the 21st century international economy and security. However, the two international organizations (IOs) have responded differently in designing and implementing strategies to combat them. NATO and the EU share not only the commonalities (overlapping membership) but also different organizational domains and structures. Which of these two organizations is more effective in formulating and implementing policies in response to cyber threats? Why do IOs respond differently to various international threats? This paper introduces a new typology of studying how institutions respond to varying threats based on fungibility of their assets and organizational adaptability. This interaction leads to four possible outcomes: effective response, institutional ineptitude, muddling through, and a stop-and-go response. The proposed framework explains why NATO has made greater advancement in cybersecurity relative to the EU and also several important conceptual and theoretical implications for the study of IOs. First, cyber threats can be more successful to foster cooperation within IOs when defined as a security rather than an economic threat. Second, policy initiation and implementation of cyber threats can be more successful if initiated by one or several members who bring it to the top of the organization’s agenda. Alternatively, policy initiation and implementation regarding cybersecurity is more difficult when driven by IO headquarters or supra-national bodies (such as the European Commission). Third, NATO’s simplified decision-making process fosters greater organizational adaptability in combating cyber threats, whereas a complex decision-making that involves multiple principals, such as in the EU, is likely to constrain the IO’s adaptability.

Key words: NATO, the European Union, Cyber Threats, Economic and Security Cooperation, Institutionalism, Organizational Adaptability, asset fungibility

IVAN DINEV IVANOV
IGOR KOVAČ
DEPARTMENT OF POLITICAL SCIENCE
UNIVERSITY OF CINCINNATI
P.O. BOX 210375
CINCINNATI, OH 45221-0375
EMAIL: IVAN.IVANOV@UC.EDU
EMAIL: KOVACIR@MAIL.UC.EDU

Draft – Please Do Not Cite Without Authors’ Permission

Paper prepared for presentation at the ISA’s 57th Annual Convention, March 15-20, 2016, Atlanta, Georgia
Introduction

The increasing threats of cyber-attacks has caused a variety of national and international responses. For example, the latest U.S. National Security Strategy adopted in February 2015 states that the country is “shaping global standards for cybersecurity and building international capacity to disrupt and investigate cyber threats.”¹ Most European Union (EU) and NATO countries similarly adopted their own cyber security strategies.² As a result, national states and international organizations (IOs) took efforts to combat cyber threats. How do IOs, like NATO and the EU, respond to cyber threats? What are their commonalities and differences? To answer this question, it is necessary to study the broader topic of organizational response to international threats and explain why IOs respond differently to varying threats.

Understanding organizational responses to international threats has major theoretical and policy implications. International organizations are often seen fairly stable and autonomous units in international relations created to specialize in a certain area of cooperation where they have the greatest expertise.³ If this perspective is correct, then NATO would be expected to approach cyber threats as traditional security threat and develop a response strategy based on this assumption. The EU, on the other hand, would approach cyber threats as legal and economic threat to the single market. Nonetheless, IOs are not always utility maximizing bureaucracies operating within their organizational silos as discussed. Often times, each of these “formally subordinated to some outside authority” structures has “a life of its own;” it tends to “universally resist complete control” and interacts with the surrounding environment (e.g. sponsors, suppliers and customers) to expand their domains and activities.⁴ Some scholars of international cooperation have highlighted that IOs are structures that display high adaptability when the rules, norms, and procedures change in a way that enables states to

² 19 of the 28 EU members have adopted national cybersecurity strategy. Similarly, 22 of the 28 NATO members have similar national security documents.
³ For example, NATO has developed expertise in dealing with traditional and novel security threats. Other IOs like the EU, the Association of Southeast Asian Nations (ASEAN), the Latin American Common Market (MERCOSUR) have specialized in dealing with cooperation on international trade, the International Organization on Migration and the UN High Commissioner for Refugees have developed expertise to deal with refugees and migration. Similarly, the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunications Union have developed expertise in communications, and others.
overcome obstacles to cooperation, which consequently ensured their survival. Others have assumed that institutions are designed to deal with specific, narrowly defined threats and when these threats disappear, and then the IOs should disappear as well.

The paper advances the argument that IOs can exhibit varying degrees of adaptability (high or low) with regard to specific threats. In some instances, they may be able to adapt to existing threats and embrace new ones, while in another instance they may not be interested or able to adapt to existing threats. Nonetheless, adaptability alone is insufficient to explain IOs’ life and death and their response to threats. Based on their areas of competency, organizations have developed a variety of resources assets, which can be deployed with varying success to different threats. If their nature allows them to be “freely exchanged by another of like nature or kind without decreasing in value,” then these assets are fungible with the regard to the specific threat. Alternatively, they are non-fungible if the latter exchange is impossible. Therefore, asset fugibility is the second variable which, along the organizational adaptability, determines the IO’s response.

To answer the broader question about IOs’ response to global threats, we focus on cyber threats due to their complexity, versatility and significant impact on economic and security life of modern societies. Additionally, we argue that, IOs’ reactions to varying threats depend on the interaction of their asset fungibility and organizational adaptability. Therefore, organizations with highly fungible assets and high adaptability toward a given threat are more likely to develop and early and comprehensive response strategy as illustrated by NATO’s response to cyber threats. Alternatively, organizations which possess fungible assets and display low organizational adaptability vis-à-vis cyber threats, tend to have a delayed and less effective response.

The presentation below is organized as follows: First, the paper introduces a new typology that explains the relationship between the organization’s assets and its adaptability applied to various threats. Second, it justifies the selection of the two cases (NATO and the EU) and surveys core policies, institutions and practices related to these two organizations’ responses to cyber threats. Third, the study compares and contrasts the EU and NATO’s response in the

---


6 In 1993 Kenneth Waltz predicted that, once the Soviet threat disappeared, NATO would gradually fade away since its “days are not numbered, but its years are.” See Kenneth Waltz, “The Emerging Structure of International Politics,” International Security, Vol. 18, no 2 (1993), 76.

context of the proposed theoretical framework. Finally, it discusses the theoretical and policy implications of the proposed model.

**Why and How International Organizations Respond to Various Threats**

How do international organizations respond to varying threats? What internal and external forces drive their response? The organizational literature offers five contending groups of explanations. According to the *hegemonic leadership* explanation, dominant nations use IOs to “incorporate potential competitors into the status quo.”8 To that end, they manage, direct and use these organizations to solve collective action problems. As a result, IOs become tools in the hands of the dominant power, which sets up the specific legal, political, economic, and social order of international interaction (e.g. *Pax Romana, Pax Britannica, Pax Americana*, etc.).9 The major problem of this perspective is that it cannot explain organizational behavior independent of the hegemonic power in cases when there is no single dominant power or when leader’s capacity to influence the organization declines due to changing distribution of power resulting from declining hegemony.10 Similarly, coordination among various interests is a difficult and cumbersome task wherein the national leader(s) have limited capacity to coordinate IOs’ activities and influence their decision-making process.

The *institutional specialization* explanation suggests a different mechanism – it argues that IOs “provide information, reduce transaction costs, make commitments more credible, establish focal points for coordination, and in general facilitate the operation of reciprocity.”11 Organizations choose to specialize in areas where they have best assets and skills – trade, financial sector, security, communications and others. Furthermore, IOs can be compared to coordination games that solve various constraints of international cooperation sometimes referred to as “dilemmas of common interests and dilemmas of common aversions.”12 By and large, organizations concerned with economic cooperation “are more likely to be successful” that security one as the latter are quite different due to their varying “types of strategic interaction.”13 Consequently, the institutional specialization literature would expect that when they fulfill their mission or when they face various internal or external constraints, international

agreements and the subsequent organizations created with them may cease to exist. The problem with the institutional specialization literature is that it underestimates the importance of domestic organizational and bureaucratic environments surrounding its members and their importance in influencing the IOs’ agenda.

The principal-agent explanation corrects for these shortcomings by arguing that IOs are tools (agents) in the hands of their principals (both institutions and individuals) who are given a broad discretion “via contingent delegation contracts” that results in significant organizational constraints. This approach emphasizes the disjuncture between what “agents want and what their principals want.” Therefore, the principal-agent can explain two important phenomena associated with IOs: First, how bureaucracies and staff within IOs can become “agents” of the states who serve as their principals, thus accounting for a response to threats driven by those agents who want to steer IOs’ response to various threats in specific directions. Second, how institutions can exhibit organizational dysfunction and inability to react effectively to threats due to varying principals’ objectives in cases when the rational actor model expects IOs to respond as efficient utility maximizers. The main problem of the principal-agent explanation is that it offers an inward focus toward various intra-organizational players within IOs (and not just the hegemon or the most powerful countries).

Unlike the principal-agent explanation, the sociological environment literature offers an outward-looking perspective which rests on two foundational pillars: First, IOs possess a high level of autonomy and operate as a separate unit independent of their principals due to the fact that they constitute autonomous bureaucracies. Second, IOs operate in a specific environment and thus act and react in response to that environment. According to this perspective IOs are purposive and rational players operating as powerful and independent actors that sometimes can have positive and transformative impact on international relations but on other occasions can display bureaucratic inefficiency, ineffectiveness, repressiveness, and unaccountability. Whereas the sociological environment perspective successfully accounts for IOs’ outside influences, this framework is inept to explain how IOs can adapt successfully to the changing environment from the inside.

---

Lastly, the organizational adaptation literature once again focuses on the internal life of IOs to explore the conditions under which they adapt to the new circumstances. It argues that adaptation depends on whether the assets are general or specific. By and large, IOs with general assets are more adaptable to new problems, whereas those IOs possessing specific assets will display high or low adaptability depending on the “obstacles or problems that members face.”18 Thus, organizational adaptability is driven by costliness to adjust organizational assets to the changing threat environment. Whereas this finding is an important addition to the literature on international institutions, it is based on a simplified explanation according to which, in general, IOs exhibit either high or low adaptability. This explanation does not take into account that organizational adaptability can vary across different international threats and might be determined by the specific environmental context in which the organizational response occurs.

Hence, the organizational adaptation framework presents several notable weaknesses. First, the rationalist assumption does not account for the bureaucratic nature of these organizations with varying degree of internal complexity which might affect their own and adaptability (i.e. some bureaucracies may be more adaptable than others). Second, the model assumes that adaptability is essential for IOs to survive. While this finding may be accurate if the threat environment changes; however, if the threat remains unchanged, then IOs with low adaptability will still remain relevant insofar as it is able to deploy their organizational assets. Thus, adaptability may be necessary but not sufficient condition for IOs to be able to respond effectively to the new threats. Third, the organizational adaptation model assumes that IOs’ general assets are highly adaptable whereas their specific assets’ adaptability may vary. However, it is not the generality or specificity of assets that determines their effectiveness in response to an international threat, but rather their fungibility, i.e. their capacity to be freely exchanged deployed when needed in response to a specific threat.19

IO’s Responses to Threats: The Importance of Asset Fungibility and Organizational Adaptability

This paper argues that IOs respond to international threats based on two key variables – the fungibility of their assets, and their organizational adaptability. As such, the model supplements existing institutionalist literature by presenting a dynamic explanation of the IOs’ response to threats – as a result of the interaction between asset fungibility and organizational adaptability. To that end, the model discussed in this section is based on three important modifications of existing literature.

Thank you so much for your interest in this paper. If you are interested to read the full paper, please contact us at ivanovid@ucmail.uc.edu or kovacir@mail.uc.edu. We will be happy to share a copy with you. Please, do not cite this paper unless otherwise specified.

Many thanks,

-- Ivan Dinev Ivanov & Igor Kovac