Working Paper

Canadian Forces Combat Camera, DND/ Caméra de combat des Forces canadiennes, MDN IS2014-5026-03

July 2021

Authors

Kristen Csenkey

Selling Simulations: The Seduction of Cold War Techno-Fetishism in a Postmodern Cyber World

Defence & Security Foresight Group

About the Author

Kristen Csenkey is a Ph.D. Candidate at the Balsillie School of International Affairs, Waterloo, Canada. Her research focuses on the management of emerging technologies, innovation, and cyber governance in Canada. She holds numerous fellowships, including with the Canadian Global Affairs Institute (CGAI) and North American and Arctic Defence and Security Network (NAADSN). She is a Women in International Security (WIIS) Emerging Thought Leader in Digital Security and was the 2020 Women in Defence and Security (WiDS)-CGAI Fellow. Kristen is a Junior Fellow with the Defence and Security Foresight Group (DSFG) and a member of the European NATO team.

ABSTRACT

The concept of a new cyber Cold War is a *hyperreality.* This paper argues that a Cold War discourse is frequently applied to cyber and cyber-related emerging technologies. It explores why this discourse is alluring to the security community as a way to understand the current state of conflict in the world. By drawing on the works of Baudrillard and others, this paper will argue that the current Cold War discourse frames the security environment, including cyber, and is based on a comfortable imaginary reality that is knowable, ordered, and familiar. This new hyperreality focuses heavily on technologies and the perceptions of their alleged uses in future conflicts.

KEYWORDS:
Emerging technologies, military technology, cyber, postmodernism, simulation.

FUNDING ACKNOWLEDGEMENT

This Working Paper is funded by the Defence and Security Foresight Group, which receives funding from the Mobilizing Insights in Defence and Security (MINDS) program designed to facilitate collaboration and mobilize knowledge between the Department of National Defence, the Canadian Armed Forces, and academia and other experts on defence and security issues. Through its Targeted Engagement Grants, collaborative networks, scholarships, and expert briefings, MINDS works and collaborates with key partners to strengthen the foundation of evidence-based defence policymaking. These partnerships drive innovation by encouraging new analyses of emerging global events, opportunities, and crises while supporting a stronger defence and security dialogue with Canadians.

Kristen Csenkey would like to thank Dr. Bessma Momani and Kersty Kearney with the DSFG and the WIIS-C leadership, especially Dr. Aisha Ahmad, for providing the opportunity to publish this paper. The author would like to extend a special acknowledgement to Lina María Zuluaga and Jill Chapman for their work in putting this initiative together and Dr. Maria Martin de Almagro Iniesta for reviewing an earlier version of this paper.

HIGHLIGHTS

- "The Cold War is over, yet the discourse on 'Great Power' politics may say otherwise. This is especially prevalent in popular discussions about cyber and cyber-related emerging technologies and the future of conflict. The uncertainty of modernity and the postmodern condition is felt within the security community. The myths surrounding emerging technologies guide the community to the belief that we are indeed experiencing a new Cold War."

- "The nostalgia for the Cold War aesthetics as a melodramatic imagination of the security community is a search for meaning and order in a cyber hyperreality where everything seems uncertain and disordered. This includes the technologies, capabilities, adversaries, strategies, operations, and the changing nature of war itself."

- For policy and decision-makers: "1) Be critical of narratives laden with Cold War commentaries, including Great Power rivalries, competition, and misguided dichotomies, especially when integrated with cyber, 2) Be wary of technological hype and fixations on technologies without understanding their capabilities in multiple contexts and their ability to go between applications, 3) Uncertainty is ok. Facing disorder is challenging, especially from a military standpoint, but addressing uncertainty with flexible frameworks that do not seek to replicate an imaginary best practice that involves an adapted model of Cold War bipolarity."

INTRODUCTION

It is hot to talk about a new Cold War, especially if you put cyber in front of it. The new cyber Cold War concept is prominent in discussions about geopolitics and Great Power competition[1]. Some[2] have argued that the Cold War discourse frames competition and technological rivalry between states, mainly the US and China and the US and Russia, in a way that fails to reflect the complexities of current conflicts and dynamics of the original Cold War. This discourse comes through in policy and strategies, especially when referring to the governance of cyber and emerging technologies. This raises questions about the security community itself and the perceptions of policy and decision-makers in this field. Mainly, what exactly is so alluring about the Cold War that the security community keeps coming back to it as a way to understand the current state of conflict in the world? More so, why is it applied to cyber, including cyber operations, cyber-related technologies, cyberspace, etc., with such conviction? This paper frames the emphasis on a new Cold War as a *hyperreality* that is heavily focused on technologies and the perceptions of their alleged uses in future conflicts. By drawing on the works of Baudrillard and others, this paper argues that the current focus on Cold War discourse to frame the security environment, and especially cyber, is based on a comfortable imaginary reality that is knowable, ordered, and familiar. Yet, this reality is a simulation that is repeated again and again and perpetuated by a focus on emerging technologies in the discourse as embedded with geopolitics.

This paper aims to present a complex exploration into the postmodern framings of defence and security policy. This paper is structured as such: first, the rationale of this paper is presented, emphasizing its importance for policy and decision-makers and members of the security community. After this, the 'postmodern condition' is described as it relates to increasing uncertainty and disorder about the state of the world (via Bauman). This uncertain condition is then linked to a discussion about simulations of reality and hyperreality tied in with emerging technologies. Following this, the seductions of free-market capitalism are brought into discussion with the meaning-making discourse that mirrors the dichotomies of the Cold War. This serves to articulate further the linkages between seductions, capitalism, and the fetishization of technologies. Baudrillard's (in)famous arguments in *The Gulf War Did Not Take Place* (1995), and *The Spirit of Terrorism and Requiem for the Twin Towers* (2002) are used to show how hyperrealities become embedded in the discourse of the security community, especially through a focus on emerging technologies. Baudrillard's arguments lead to a discussion highlighting how this perception fetishizes technologies and is perpetuated by myths based on capitalist and consumerist intents. The last section discusses the current understanding of emerging technologies and cyber in Canada from a military perspective in policy language in *Strong, Secure, Engaged: Canada's Defence Policy* (2017) (SSE). The paper concludes with a 'translation' of the discussion by describing three tangible considerations for policy and decision-makers.

[1] See, for example, Gladstone, R. "How the Cold War Between China and U.S. Is Intensifying," *New York Times*, 2021, Sanger, D. "Once, Superpower Summits Were About Nukes. Now, It's Cyberweapons," *New York Times*, 2021, Feffer, J. "The Cyber Cold War Is Here", The Nation, 2021, and Segal, A. "The Coming Tech Cold War With China Beijing Is Already Countering Washington's Policy," *Foreign Affairs*, 2020.

[2] For example, Bisley, N. "The China-US rivalry is not a new Cold War. It is way more complex and could last much longer," *The Conversation*, 2020.

IMPORTANCE OF METAPHORS AND ANALOGIES

A postmodern deep dive into cyber and emerging technologies might seem beyond the scope of a policy audience. Perhaps it may seem too complex and abstract for consideration in decision-making. However, it is not as abstract or removed from policy and decision-making as one would assume. This is because discourse can shape organization, practices, methods, and strategy, or the 'reality' of policymaking.

The discourse about cyber, including threats, security, and space, shapes and is shaped by the definition of 'reality'. Dunn Cavelty (2013) shows that various actors, including state and non-state actors, seek to assert themselves within this definition process. Part of this process involves the use of metaphors and analogies. Metaphors shape 'reality', what is 'known', or imagined, about cyber. For example, imagining cyberspace as a 'frontier' associates the concepts of unruliness and lawlessness with the need for order within this domain (Dunn Cavelty 2013). Sulek and Moran (2009) show how analogies, such as a Cyber Pearl Harbour, cyber Cold War, and cyber 9/11, etc., can inform future cyber strategies. In their analysis of the cyber Cold War analogy, Sulek and Moran (2009) show that it is "primarily anchored in the idea that powerful nation-states are competing for influence and power without resorting to a direct conventional or nuclear war" (8). Nevertheless, their comparison of the similarities and differences between the 'actual' Cold War and a cyber Cold War does not adequately explore the underlying fixations, spectacle, and seductions of this period and how this shapes decision-making and strategy. What is needed is a more nuanced understanding of why this analogy exists, its context, and what it says about the security community's goals, fears, and choices.

Although the threat environment has changed since the Cold War, narratives drawing on this period still permeate policy and influence decision-making. These narratives frequently imply a level of certainty, calculability, and relative stability of an apparently bipolar world. The intricacies of current conflicts and threats require a more nuanced understanding, and a postmodern approach may help the security community better understand these complexities (Dunn Cavelty and Mauer 2009). This means understanding and facing the 'new' 'cyber' Cold War discourse and its impact on cyber and defence strategy for policy and decision-makers. This process starts by delving into the postmodern condition and the search for meaning and stability.

THE POSTMODERN CONDITION

Modernity is characterized as a search for meaning, order, and stability. Prior to the influence of globalization and neoliberalism, this search was usually answered in the West by the state, church, and/or family, whereby citizens found stability and identity. Large-scale globalization and neoliberalism starting in the 1990s opened up the world to the possibility of choice. It presented individuals with the freedom to make meaning through their own choices. The corresponding retreat of the state gave individuals a diversity of options to find meaning, yet this freedom resulted in instability. According to Bauman (1997), this instability results from a sense of insecurity, uncertainty, and the constant search for meaning outside of the traditional channels. This is the postmodern condition, specifically the power of other actors outside and including the state, to control individuals' options for choice. As a result, individuals are without traditional criteria for ascribing identity or achieving meaning in life.

Thus, they search elsewhere for meaning and new lifestyles. These identity-making and consumer-oriented options are coloured with capitalism and aim to 'seduce' individuals into consumerism to ease the overwhelming sense of uncertainty. This uncertainty is fuelled by capitalistic dreams that can promise meaning and fulfillment.

In *Liquid Life*, Bauman (2005) characterizes postmodern life as a constant struggle of reinvention and a search for meaning. This search for meaning and purpose can be applied to any part of society whereby the state's traditional role is in flux and new possibilities are sought. Globalization has changed the interactions and organization between people, and as a result, changed the constructs that traditionally bind people to a state. The subsequent uncertainty, or liquidity of meaning and belonging in the modern world, has led to many responses by diverse actors outside of the traditional state-focused approach. Responses to this liquidity must mould tangible meaning for individuals to choose; it must also provide structure, identity, meaning, and can be flavoured with capitalism, or as argued elsewhere (see Csenkey 2018), populism and nationalism. States can use these flavours to bolster state-serving practises, for example, by structuring fear of the 'Other' in border security and national security policies (Csenkey 2018; 2020; Bauman 2006). For Bauman, individuals are left with no strings to grasp from the past as they buy into these new capitalist dreams.

Unlike Bauman (2005), Baudrillard (1994) does not see globalization and neoliberalism as the end of history (Fukuyama 1992) or identity. New meanings and lifestyles are not necessarily new — they can be rebranded and sold in new ways with mixed flavours — the 'old wine, new bottles' approach. For Baudrillard, the postmodern condition includes all ideas from the past. These ideas, however, are now negotiable and are included in the mix of histories and simulations to be seduced by.

The postmodern condition is essential to understand because it is tied inextricably with the simulations that make postmodern life a reality. Uncertainty about order, meaning, and the search for identity and stability in a globalized world can be rebranded and sold as answers. These answers can be crafted as realities (vis-a-vis Baudrillard). However, as we shall see, these realities are simulations, and simulations of simulations, and simulations of the real.

SIMULATIONS OF THE REAL

Simulations are reality without reality. The postmodern condition is characterized by simulations and hyperrealities (recall Baudrillard). These simulations and hyperrealities guide perceptions of reality, including choices, identities, and governance practices.

Using Baudrillard's (1983) example, imagine the creation of a map. The mapping of a territory, including drawing its borders, natural features, and parcelling out associated sovereignty claims, is based on a reality. This reality is based on geography, history, and the real world — yet it is only a simulation of the real. When the reality that the simulation is based on is removed, all following reproductions are based on the simulation itself. What is left is a 'hyperreality' or a *simulacrum*. Baudrillard describes this as a model of a real without the original reality. For Baudrillard:

"[t]he real is produced from miniaturized units, from matrices, memory banks and

> command models - and with these, it can be reproduced an indefinite number of times. It no longer has to be rational since it is no longer measured against some ideal or negative instance. It is nothing more than operational. In fact, since it is no longer enveloped by an imaginary, it is no longer real at all. It is hyperreal: the product of an irradiating synthesis of combinatory models in a hyperspace without atmosphere." (1983: 3).

Hyperrealities are not duplicates or imitations of reality, nor are they representations. Representations assume that the sign and the real are equivalent. *Simulacrum*, or hyperrealities, are simulations of reality, reflections that mask or in some way pervert reality. It masks it in such a way that it does not look like reality anymore and bears no relation. Cyber is a hyperreality — it is a simulation of the real.

Inscribing Reality, or how to Govern Technologies

Cyber is a hyperreal space; it has intangible and tangible pieces, is interacted by diverse users, technologies, and operates in different contexts. From a military perspective, this is problematic. The liquidity of the postmodern condition affects military frameworks because it creates uncertainty about structure, order, and rationale. This is further complicated by the plethora of actors, including new adversaries and their motives and strategies, operating in this space. Additionally, new technologies, especially those outside of a defence context, are challenging to govern. In combination, all of these factors result in instability. One such way is to stabilize the unstable, solidify the liquid uncertainty, and define reality through inscription.

The complexity and uncertainty associated with cyber and emerging technologies operating in this space can be made tangible, and therefore governable through inscription. For Latour (1987), part of this process is through *inscription devices*. Reality is made stable through the inscription of meaning onto things and concepts. When reality is made stable, it is comparable, combinable; it can be debated, calculated, and diagnosed. Part of this inscription process involves making and using information. In *Seeing Like a State*, Scott (1998) argues that states craft ways to imagine the world as easier to govern. States do this by making people, processes, things, regions, etc. quantifiable, or easier to govern through current systems. For example, assigning a person a SIN or giving areas of land postal codes. This, in turn, modifies the perception of these 'things' and feeds into the design, enforcement, and retention of governance through a specific lens. These are *inscription devices* enabling information to be created about concepts and things. This information is used and funnelled through '*centres of calculation*' whereby it is understood in relation to other information (Latour 1987). In these centres of calculation, the information is manipulated for use, including understanding its effects on other information.

Inscriptions accumulate, and this makes them powerful. The more information is gathered, manipulated, computed, and used via centers of calculation, the more legitimate they become. This information is transformed into plans and strategies, whereby legitimacy, and therefore power, is ascribed to those who seek to govern. When cyber-related emerging technologies are inscribed with a reality through information about them from a specific context, it makes them governable. This

paper focuses on understanding the realities cyber technologies are inscribed with and how and why they seduce the security community.

SEDUCTION: MARKETING IDENTITY AND MEANING

Although 'free' to choose meaning and lifestyles, there is a perpetual uncertainty about the world (Bauman 1997; 2005). Some of this uncertainty is nested in technologies, their uses, users, capabilities, contexts, etc. Globalization saw a decline in metanarratives and grand theories, especially those held and perpetuated by traditional actors like the state. Technologies can be seen as part of a regime of globalization. Although there is anxiety about technologies, the associated narratives provide some recentering and restoration of meaning and choice. For Baudrillard, this is power which he calls seduction, and it resides in the representation of the visible and invisible and making it consumable. Society is organized around the logic of consumption. Consumerism has brought some certainty and stability to the liquid uncertainty of the globalized world. One of the comforting aspects of consumerism is that it is limitless (Baudrillard 1998 [1970]). This means that there are never-ending promises and pleasures. Society's appetites will constantly grow and seek new products as a consuming community. In other words, it is a society driven by consumerism (Bauman 1992) and a postmodern world of simulations and hyperrealities (vis-a-vis Baudrillard). The key to fulfilling and perpetuating these endless consumeristic needs is through seduction, primarily through the production of imagery and information.

According to Baudrillard (1990 [1979]), seduction is "the strategy of appearance" (7, 8), including over imagery. Seduction supposes an order of things based on something beyond reality, although it appears to offer it. The seduction of a reality that offers stability, including familiar imagery, meaning, and aesthetics, drives the desire to 'buy-in'. The seduction of meaning through imagery was on display in a newly 'experienced' way during the technology theatre of the Gulf War.

THE TECHNOLOGY THEATRE OF THE GULF WAR

The Gulf War could be seen as a high-tech war, a 'clean' war — where technologies were used to engage in an efficient and modern conflict whereby the state with the most advanced technologies would win and suffer less casualties. This would act as a deterrent to other adversaries to engage in future conflicts. This high-tech war was seen and 'experienced' through new media, with new visuals and aesthetics. 'Real'-time footage from US bombers in the air and from cameras on the ground allowed the 'audience' to 'see' the action. Nevertheless, this vision of a 'virtual,' high precision war was not real. Baudrillard argues in his 1995 piece, *The Gulf War Did Not Take Place*, that what the 'audience' or viewers saw through the media in 1990 -1991 was not the reality of the Gulf War. What was seen was, in fact, a simulation of a real war on television. What was seen and heard did not happen — that war was not real and did not occur. Baudrillard (1992) argues that the media provides a simulation because it is an imperfect representation of what happens in the world and the representations of the real world.

From this simulation of high-tech war, a new hyperreality was created — one that looks like the simulated reality without the original. This has altered the perception not only of what happened

during the Gulf War but following conflicts. At the heart of this hyperreality is a fixation with technology. This fixation plays out as a '*technology theatre.*'

Technology theatre builds off Schneier's (2003) original understanding of the '*security theatre*.' Simply, the security theatre is doing 'things' to make reality feel secure without actually addressing the causes of insecurity or threats. Heightened airport security infrastructures after 9/11 are an often-cited example of the security theatre. The technology theatre is similar because it also attempts to build a sense of security through interventions that appear to solve a problem. McDonald (2020) defines technology theatre as "the use of technology interventions that make people feel as if a government — and, more often, a specific group of political leaders — is solving a problem, without it doing anything to actually solve that problem." For McDonald, the technology theatre is a distraction, a political tactic used to make governments appear to be making progress in solving an issue. For example, this issue could be attempting to address the outbreak of COVID-19 through contact tracing applications. This paper sees the technology theatre a bit differently. Instead of a largely political tool, the technology theatre within the context of military operations is where the hyperreality of war takes stage, with high-tech weapons on show in a way that further reinforces the simulated reality of conflict. Both the technology and the security theatres build on the visible aspect of doing 'things' to address problems — even if these 'things' are performative instead of constructive.

The Spectacle of the Hyperreal

Unlike Baudrillard's controversial statements in *The Gulf War* (1995), in *The Spirit of Terrorism and Requiem for the Twin Towers* (2002), Baudrillard argues that 9/11 did happen. Yet, he argues that there were intangible unrealities that collapsed into each other as 9/11 became an exchange of symbolic violence presented through the media (ibid. 2002). This was different from what was 'seen' during the Gulf War. The terrorist attacks in 2001 on the World Trade Center destroyed the physical structures and the symbolic object. This occurred as a 'spectacle,' a 'fascination' with the image and its symbolism. More specifically, "[t]he image consumes the event, in the sense that it absorbs it and offers it for consumption" (Baudrillard 2002: 21). This is different from McLuhan's (1964) idea that 'the medium is the message.' Hyperreality does not distinguish between the medium or the message — the two can no longer be determined as distinct — they collapse into each other (Baudrillard 1994). Technologies and their content are not reality. Hyperreality, simulated imagery, and inscribed technologies and information are part of the technology theatre and are created by spectacles to be seduced by.

For Baudrillard, the Gulf War was a drama of a war whereby Western power and ideas of modernity, democracy, and order were fully displayed. This theatre performance was a hyperreality because the war appeared orderly, precise, 'consensual,' and certain. The viewers at home could 'experience' the visuals and an impression of war without the original at their leisure. The Gulf War was an "...unreal war in which the over-dimensioned technical power, in turn, over-evaluates the real forces of an enemy which it cannot see" (Baudrillard 1995: 80). The current perceptions of war were shaped by this simulation and are now hyperrealities. The consumer viewers' experience of war is mundane and tied with leisure and the expectation that high tech will win wars. The consumer has many options to experience this hyperreality, including imagery and aesthetics imbued with meaning.

The technologies within this theatre were inscribed with information and meaning that feeds into and reinforces the performance itself. These *inscription devices* (recall Latour 1987) are then reinforced by hyperrealities seen in visuals on television and in 'real' time and played a role in the confusion of the real and the hyperreal, including a fetishization of technologies.

FETISHIZING TECHNOLOGIES: THE PLEASURES OF THE REAL MYTHS

In this context of this discussion, a fetish is a consumer object. It is something to be seduced by through consumption (Baudrillard 1998 [1970]). As previously discussed, consumerism is intertwined with the postmodern condition and hyperreality. Technologies can be fetishized and turned into objects of desire and fantasy-building. As argued by Baudrillard (1995), this was seen during the Gulf War, where an emphasis on technologies as winning hyperreal wars is pivotal to how we perceive the future of conflict. The technology theatre places technologies at the center of the stage to perform military solutions to problems.

Circling back to the focus of this paper, what is to be done about simulations, hyperrealities, theatres, and fetishisms? Why does the security community fixate on Cold War discourse, fetishize technologies, and become seduced by the hyperreality of a cyber Cold War? Ang's (1989) work on *melodramatic imaginations* brings us towards some possible answers. Drawing on Ang (1989; 1996), 'real' 'pleasures' can be fulfilled by fantasies or myths. These are realities in themselves, albeit hyperrealities, and this is a place to look for some insight into the fixation with the new Cold War discourse.

Pleasures are not satisfactions; they are instead longing for a past that can include a perceived future. This future can also be a perceived past — or a hyperreality — it can be a present, but in all cases, it is connected to the fiction of positions, solutions, feelings, and structures (Ang 1989). In other words, there is pleasure in fictional representations of reality or the *melodramatic imagination*. Identity and meaning within these imaginations are fluid and are given meaning when performed. Recalling Butler's (1990) arguments about the performativity and fluidity of gender, these identity performances occur within specific contexts. To situate this argument in this paper: technology theatres are where and how identities are performed, and this gives and reinforces its meaning. These performances and melodramatic imaginations are nested in nostalgia for the Cold War era, or more specifically, the order, meaning, and identity ascribed within the binary of bipolarity. This is the pleasure of the techno-fetish.

The nostalgia for the Cold War aesthetics as a melodramatic imagination of the security community is a search for meaning and order in a cyber hyperreality where everything seems uncertain and disordered. This includes the technologies, capabilities, adversaries, strategies, operations, and the changing nature of war itself. Nostalgia, myths, and simulations go hand-in-hand in this case:

> "When the real is no longer what it used to be, nostalgia assumes its full meaning. There is a proliferation of myths of origin and signs of reality; of second-hand truth, objectivity and authenticity. There is an escalation of the true, of the lived experience;

> a resurrection of the figurative where the object and substance have disappeared. And there is a panic-stricken production of the real and the referential, above and parallel to the panic of material production. This is how simulation appears in the phase that concerns us: a strategy of the real, neo-real and hyperreal, whose universal double is a strategy of deterrence." (Baudrillard 1983: 12).

Drawing on Mosco's (2005) description of the *Digital Sublime*, to contextualize myths about technologies, myths "offer entrance to another reality, a reality... characterized by the promise of the sublime" (3). The sublime and sublime icons are sources of "utopian visions" (ibid: 6) "mutually constituted ...out of the interconnected realities…." (ibid: 10). Myths are not just distortions of reality — they are a form of reality and give meaning to the incomprehensible, allow us to cope with overwhelming problems, and create comfortable and consensual visions.

Myths are central to understanding cyber hyperrealities and new Cold War discourse. Examining myths about technologies reveals the desires and the hidden configurations of power nested in neoliberal practises. Myths are enacted and continually contribute to constructing mythic 'things,' theatres, and performances. In the next section, we apply theory to practice.

COLD WAR MYTHS TODAY

The Cold War is over, yet the discourse on "Great Power" politics may say otherwise. This is especially prevalent in popular discussions about cyber and cyber-related emerging technologies and the future of conflict. The uncertainty of modernity and the postmodern condition is felt within the security community. The myths surrounding emerging technologies guide the community to believe that we are indeed experiencing a new Cold War. This is a *melodramatic imagination* to find pleasure and comfort in the knowable and a past real (or a perception of a past), where technologies were seen as tangible, and the wars' happened.' These pasts and futures are ideas and aesthetics for sale. Myths are seductive, and "[i]n the real world, the development and deployment of technologies have generated their own mythic structures, borrowing from much older ideas and bringing these together with new ideas have produced myths repacked for our time" (Burnett et al. 2009: 1-2). Myths support and sustain consumerism, creating identity, structures, institutions, and a complex interplay of understandings. This is important to understand because it shapes everyday lives, lived experiences, uses of technologies, and shapes world views and power relations.

In defence policy, these myths and pleasurable hyperrealities are reinforced. In SSE, for example, new Cold War nostalgia is visible and mixed with the hyperreality of cyber:

> "The *re-emergence of major power competition* has reminded Canada and its allies of the importance of deterrence. At its core, deterrence is about discouraging a potential adversary from doing something harmful before they do it... Deterrence has traditionally focused on conventional and nuclear capabilities, but the concept is also increasingly relevant to the space and cyber domains." (emphasis added, DND 2017: 50).

Discussions about major power competition, deterrence, and geopolitical technology races are new

Cold War discourse. SSE describes the changing nature of warfare due to the proliferation of weapons, hybrid tactics, terrorism, among other factors. In the subsection, "The Re-Emergence of Deterrence," the changing global security environment is described as a "*return of major power rivalry*, new threats from non-state actors, and challenges in the space and cyber domains have *returned deterrence to the centre of defence thinking*" (emphasis added, DND 2017: 55).

Linking these concepts back to Baudrillard's arguments in *The Gulf War* (1995), war is a technology theatre whereby the heavy use and the public display of high-tech weaponry in a conflict fetishize technologies. For Baudrillard (1995), the Gulf War legitimized the logic of deterrence. One of the problems with deterrence is that it assumes that everyone is on the same strategy page with equal access to technology and weaponry. It assumes that there is a result of escalation and is seeded in assumptions about deterrence itself. For Baudrillard (1995), the Cold War was based on the realist logic of deterrence. This has become a hyperrealist logic of deterrence whereby the real is deterred by the virtual. This logic has fundamentally changed war — it has made war abstract, beyond the imaginary, so that it becomes an unreality that is the reality.

Uncertainty about the future is perceived as uncertainty about technological capabilities and their alignment with current understanding and conflict strategies. SSE states:

> "Technological developments point to a future of defence that is expected to be vastly different than today, with a greater emphasis on information technologies, data analytics, deep learning, autonomous systems, advancements in the electromagnetic and cyber domains, as well as a range of transformative technologies, from quantum computing to synthetic biology. Any number of these advances has the potential to change the fundamental nature of military operations." (55).

According to Baudrillard, the technology theatre and the conflict that followed the Gulf War are not about politics. Specifically, they are not the virtual version of the Clausewitzian concept of the 'absence of war by other means.' Cyber conflicts, or as Baudrillard refers to them as 'electronic wars', do not have political objectives because:

> "It functions as a preventative electroshock against any future conflict. Just as in modern communication, there is no longer any interlocutor, so in this electronic war there is no longer any enemy, there is only a refractory element which must be neutralized and consensual." (1995: 84).

In crafting policies to understand and strategize the future of conflict, it is crucial to recognize the role that information plays in inscription devices and the centres of calculation (Latour 1987). The manipulation and use of information about technologies ascribes legitimacy.

CONCLUDING REMARKS: TRANSLATION, PLEASE

To summarize the theoretical portion of this paper: the Cold War was a perfectly conformable simulated reality to build into a simulacrum. There was order in the Cold War: there was duality, dichotomies, bipolarity. Yet, this was not the lived reality of the Cold War, but a melodramatic imagination, where the imagery and perception of advanced technologies are fetishized as the answer to solving conflicts.

This paper has engaged in a complicated discussion about how technologies are framed within certain realities, used to craft hyperrealities, and perpetuate mutually constructed myths about conflict in the world. If the reader is skimming to the end of this paper to arrive at the 'so-what' value, or to find some translation for this postmodern-heavy content, then it is presented in this section. The answer to the question: *what does this mean for decision-makers*? is presented here as simply, proceed with caution and do it in three ways:

1) Be critical of narratives laden with Cold War commentaries, including Great Power rivalries, competition, and misguided dichotomies, especially when integrated into the cyber environment. Multiple actors exist and operate in the world, each with different strategies, linkages, and goals. Competition between actors may assume equal access to technology or similar strategies, but it is not always the case.

2) Be wary of technological hype and fixations on technologies without understanding their capabilities in multiple contexts and their ability to go between applications. Technologies can be sold for more than what they are, and they may also assume compatible uses across multiple contexts.

3) Uncertainty is ok. Facing disorder is challenging, especially from a military standpoint, but addressing uncertainty with flexible frameworks that do not seek to replicate an imaginary best practice that involves an adapted model of Cold War bipolarity.

REFERENCES CITED

Ang, I. *Watching Dallas: Soap Opera and the Melodramatic Imagination*. London: Routledge, 1989.

---. *Living Room Wars: Rethinking Media Audiences for a Postmodern World*. London: Routledge, 1996.

Baudrillard, Jean.

---. *The Illusion of the End*. Wiley, 1992.

---. *Simulacra and Simulation*. University of Michigan Press, 1994.

---. *The Gulf War Did Not Take Place*. Indiana University Press, 1995.

---. *The Consumer Society: Myths and Structures.* Revised edition. London: SAGE Publications Ltd, [1970] 1998.

---. *The Spirit of Terrorism and Requiem for the Twin Towers*. Verso Books, 2002.

Baudrillard, Jean, and Paul Foss. *Simulations*. New York: Semiotext (e), 1983.

Baudrillard, Jean, and Brian Singer. *Seduction*. New World Perspectives, [1979] 1990.

Bauman, Zygmunt. *Postmodernity and its Discontents*. Polity Press, 1997.

---. *Liquid life*. Polity Press, 2005.

---*Liquid Fear*. Polity Press, 2006.

Bisley, N. "The China-US rivalry is not a new Cold War. It is way more complex and could last much longer," *The Conversation*, 2020.

Burnett, Judith, Peter Senker, and Kathy Walker, eds. *The myths of technology: Innovation and inequality*. Vol. 46. Peter Lang, 2009.

Butler, J. "Performative acts and gender constitution: an essay in phenomenology and feminist theory", in S. Ellen (ed.) *Performing Feminisms: Feminist Critical Theory and Theatre*. Baltimore, MD: The Johns Hopkins Press: 270–82, 1990.

Csenkey, Kristen. "Illiberal Democracy and Reimagined Nationalism: Hungary's Anti-NGO Law and Border Security Policies", unpublished major research paper, Waterloo: Wilfrid Laurier University, 2018.

---. "On the Uses of Populism and Illiberal Democracy: Fences, Border Hunters, and Identity", Canada Europe Dialogue on Democracy project, Centre for Global Studies, University of Victoria, 2020.

---. "Protecting Canada and improving cyber defence: three challenges", *The Hill Times's Special Edition: Defence Policy,* 2021. https://www.hilltimes.com/2021/05/24/protecting-canada-and-improving-cyber-defence-three-challenges/298196

Department of National Defence. *Strong, Secure, Engaged: Canada's Defence Policy*. Canada, 2017. https:/ www.canada.ca/content/dam/dnd-mdn/documents/reports/2018/strong-secure-engaged/canada-defence-policy-report.pdf

Dunn Cavelty, Myriam. "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse." *International Studies Review* 15, no. 1 (2013): 105-122.

Dunn Cavelty, Myriam, and Victor Mauer. "Postmodern intelligence: Strategic warning in an age of reflexive intelligence." *Security Dialogue* 40, no. 2 (2009): 123-144.

Feffer, J. "The Cyber Cold War Is Here", *The Nation,* 2021.

Fukuyama, Francis. *The end of history and the last man*. United Kingdom: Penguin Adult, 1992.

Gladstone, R. "How the Cold War Between China and U.S. Is Intensifying," *New York Times*, 2021.

Latour, Bruno. *Science in action: How to follow scientists and engineers through society*. Harvard University Press, 1987.

McLuhan, M. *Understanding Media: The Extensions of Man*. London: MIT Press, 1964.

McDonald, Sean. “Technology Theatre.” Waterloo: Centre for International Governance and Innovation, 2020. https://www.cigionline.org/articles/technology-theatre#:~:text=Technology%20theatre%2C%20here%2C%20refers%20to,to%20actually%20solve%20that%20problem.

Mosco, Vincent. *The digital sublime: Myth, power, and cyberspace*. MIT Press, 2005.

Sanger, D. “Once, Superpower Summits Were About Nukes. Now, It’s Cyberweapons,” *New York Times,* 2021.

Schneier, Bruce. *Beyond fear: Thinking sensibly about security in an uncertain world*. Copernicus Books, 2003.

Scott, James C. *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press, 1998.

Segal, A. “The Coming Tech Cold War With China Beijing Is Already Countering Washington’s Policy,” *Foreign Affairs*, 2020.

Sulek, David and Ned Moran. “What analogies can tell us about the future of cybersecurity.” *The virtual battlefield: Perspectives on cyber warfare* 3 (2009): 118-131.