Western Kentucky University

TopSCHOLAR®

Honors College Capstone Experience/Thesis **Projects**

Honors College at WKU

2020

Baudrillard and the Viral Violence of Cyber Security

Alex Rivera Western Kentucky University, alex.mckenzie.rivera@gmail.com

Follow this and additional works at: https://digitalcommons.wku.edu/stu_hon_theses



Part of the Other History Commons, Philosophy Commons, and the Political Science Commons

Recommended Citation

Rivera, Alex, "Baudrillard and the Viral Violence of Cyber Security" (2020). Honors College Capstone Experience/Thesis Projects. Paper 844.

https://digitalcommons.wku.edu/stu_hon_theses/844

This Thesis is brought to you for free and open access by TopSCHOLAR®. It has been accepted for inclusion in Honors College Capstone Experience/Thesis Projects by an authorized administrator of TopSCHOLAR®. For more information, please contact topscholar@wku.edu.

BAUDRILLARD AND THE VIRAL VIOLENCE OF CYBER SECURITY

A Capstone Project Presented in Partial Fulfillment
of the Requirements for the Degree Bachelor of Arts
with Mahurin Honors College Graduate Distinction at
Western Kentucky University

By

Alex M. Rivera

May 2020

CE/T Committee:

Professor Michael Seidler

Chad Meadows

Copyright by Alex M. Rivera 2020

ABSTRACT

This paper explores Jean Baudrillard's theorization on war and communication, connecting it to recent developments in the field of cyber security. With the important elevation of military forces such as the United States Cyber Command, critical theory needs to interrogate the increasing stature and seriousness of the cyber domain in global military strategies. Baudrillard's critique shifts the focus from simple military strategies to the globe's consumption of the information that is offered by the global information complex. This paper explains the nuances of violence surrounding the exchange of media surrounding war, criticizing both pro-war and anti-war stances, to examine the difficulties with traditional solutions to conflict. Drawing directly from Baudrillard's work as well as modern academic publications that apply his ideas to newer conflicts, this paper seeks to revitalize critiques of semiotic warfare and bolster their contextualization to current events in cyber security in order to keep Baudrillardian thought relevant.

VITA

EDUCATION

Western Kentucky University, Bowling Green, KY
May 2020

B.A. in Philosophy – Mahurin Honors College Graduate

Honors Capstone: Baudrillard and the Viral Violence of Cybersecurity

Newton High School, Newton, KS May 2016

PROFESSIONAL EXPERIENCE

Ridge High School, NJ April 2018 –

Director of Debate Present

Roosevelt Institute, NY August 2018 –

Research Internship August 2019

CONTENTS

Abstract	ii
Vita	iii
The Viral Nature of Cyber War	1
Cyber War and the Extermination of Event	11
Toward an Illusory Reading of Cyber War	18
References	22

THE VIRAL NATURE OF CYBER WAR

In the beginning of Baudrillard's book Simulacra and Simulation, he describes a fable written by Jorge Luis Borges which illustrates the quest of an empire's cartographer to make a wholly detailed map of their territory (Baudrillard, 1981). He made a map so precise that it was no longer restricted to any sheet of paper; the sharp black lines imposed themselves on the territory itself, striping paint over the real land with its transcription. The map, a simulation of the area, subsumed the reality of the territory within it. If the empire were to crumble, the deserts would have also frayed like worn sheets, because there was no longer any distinction to be drawn between the map and the real. However, even if the citizens of the empire, duped by the authenticity of the simulation, navigated the region solely by the painting of the land below them, they would still hold some reference to the real object being represented. For Baudrillard this allegory can no longer hold true; we have surpassed the charm of an illusion that strictly mimics something real and have transitioned into a hyperreal society (Baudrillard, 1981). This is characterized by a closed loop where simulations, which are supposed to represent a real-world process or object, instead strictly represent other simulations. The collapse of the real marks a cohesive system of illusions that are more real than reality itself.

The 1999 documentary on Fox TV, *Dangers on the Internet Highway:*Cyberterror, is perhaps when cyber war's place in the domain of hyperreality became

obvious (Debrix, 2001). This informative piece conjures up a fictitious scenario to lament the Armageddon-like consequences of a cyber-attack on the United States. Americans are killed in airplane crashes as computers malfunction, and many more perish when electrical grids shut off and nuclear power plants meltdown. Determining whether attacks were sponsored by government or non-state actors is difficult and the United States can do little to find the actor(s) and stop the attacks. The message viewers are left with is clear: there is danger from uncertain enemies, and we must expand the scope of our conflict to compensate (Debrix, 2001). What characterizes hyperreality, the uncertainty of an event and its images becoming more real than reality itself, describes what is at play here. The threat of terrorism is no longer relegated to any particular location, person, or ideology, but demands to be real by virtue of its innate possibility. Media portrayals generate a threat that is always imminent, capable of weaponizing the cell phones and laptop computers carried on our bodies. As the threat is decentralized and always unknown, militaristic response is decided by potentialities rather than any actual event (Cristiano, 2018). The conflict being waged is just as virtual as the threat itself; war games are routinely conducted by the United States military to respond to challenges with no historical analogues, such as a total electrical grid collapse. This absurdity is illustrated by NATO's Locked Shield exercise in 2016, which designed the fictional country Berylia to be the focal point of cyber-attacks (Cristiano, 2018). Yet, the fictional design of games like these ironically maintain the integrity of cyber war; the inherent uncertainty of cyber war, due to the difficulty of attributing actors, and the viral nature of modern war where information is exchanged like a virus, nullifies the requirement for a concrete perpetrator or victim. No real perpetrator exists to compare with Berylia; its

simulation is the only referent. The games and the media coverage being produced are not distinct entities from the conflict they mirror. They do not afford that degree of distance. They are the war being waged. In a desperate attempt to demonstrate its reality, the military has paradoxically proved the existence and legitimacy of a nonexistent cyber event by elevating Cybercommand to its combatant command status in the United States military posture. It has transcended the level of second order simulation by being the chief influencer over reality; the viral mediation of the nonevent has rendered the question of its own existence irrelevant to how the conflict is conducted. In Baudrillard's world, there is no distinction to be drawn between military clashes, war games, and the imposed global system of semiotic exchange. They belong entirely to the realm of hyperreality; a violent closed circuit of self-referential simulations.

Some national security experts could leverage a fair criticism against

Baudrillard's proclamation that such a cyber war is not real. Since crimes like cyber
intellectual property theft and election hacking have been thought to happen quite
consistently, it is important to clarify exactly what is being argued here. First, when
Baudrillard wrote his series of essays on the gulf war titled, *The Gulf War did not take*place, he was not insinuating that there was no military presence in the Persian Gulf but
was instead criticizing its lack of reality. He argues that the war "[...] has been
envisaged, programmed, and anticipated so much that it does not even need to take
place", but "[...] even if it takes place in "reality," it will already have virtually taken
place and thus it will not be an event" (Baudrillard, 2003). The world had already been so
thoroughly exposed to vivid simulations and predictions of the Gulf War, which was so
distant that the west would only ever experience it from the television anyway, that there

would be no new event to speak of. A similar bombardment of simulations could be said of cyber war, which has not desensitized society to a catastrophe but instead has oversensitized us into making panic completely normal (Debrix, 2001). This is why media representations of cyberterrorism have become ever more spectacular to capture our attention. Yet, it also ensures that any real cyber event that does not match the level of violence captured in these simulations will be met with apathy and denial; a simple generator going haywire will fail to be much of an event at all (Debrix, 2001). Moreover, military doctrine has been set up to achieve comparative cyber-superiority (a combination of defending friendly assets and attacking adversary assets) based upon simulations that are ahistorical. The theoretical possibility for a hack that collapses societal assets and creates mass casualties does not seem to justify the simulation's relation to reality.

There is something profoundly important, yet completely predictable about the elevation of Cybercommand. It marks perhaps the most substantial nod of legitimacy that the domain of cyber war has ever received. With only ten unified combatant commands in existence, it has matched the importance of nuclear deterrence and geographical counterbalancing. However, for Baudrillard, this was always the direction the conflict was heading; a necessary component of the event manufacturing process. One may inquire what exactly is being manufactured, since there must be some events that are more real than others? The search for specific cyber threats, which may appear to have more justifiable evidence than the others, misunderstands the new nature of war. As Baudrillard writes in his essay *War Porn*, "[...] it does not help to know whether the images are true or false. From now on and forever we will be uncertain about these images. Only their impact counts in the way in which they are immersed in the war"

(Baudrillard, 2006). Here, Baudrillard differs from many realists or academics from the Critical Security Studies discipline who are interested in whether a particular nation-state is a cyber threat. The focus on instances of when a country's cyber capability can be chalked up to media hype or not, would be a simple materialist recounting of threats that is equally complacent in the illusion. For Baudrillard, it is far more about how the images themselves function as warfare, with distinct goals from usual geopolitics. In the essay, he describes a short story from Patrick Dekaerke that depicts the images that arose from the horrendous conditions of the Abu Ghraib prison in Baghdad during the United States invasion of Iraq. American soldiers forced Iraqi's to strip naked and sodomize pigs while taking photos of the sexual humiliation (Baudrillard, 2006). The images were sent to their villages and families, conducting the violence of symbolic eradication. "[...] the goal of the war is not to kill or to win [...]", writes Baudrillard, "[...] but abolish the enemy, extinguish [...] the light of his sky" (Baudrillard, 2006). Here lies a motivation for violence that exists beyond something that is strictly material, but instead constitutes a kind of symbolic warfare. It did not help to know whether the images from the prison were fabricated or not. They were an ammunition of war, a repugnant display of symbolic eradication, and the gun was the global media apparatus, laying the images of horror bare for all to witness. Yet, images of war like these are rare for a reason, and although they may have been weaponized for symbolic domination, they end up producing the opposite effect by serving as their own criticism of symbolic exchange.

The closer one comes to mastering the image, the more catastrophic its reversal will be, and that is why symbolic victory must stray from completeness if it wishes to maintain itself. Violence and humiliation this grotesque illustrates the limits of power,

which is incapable of dealing with itself, and instead returns to humiliate its own wielder (Baudrillard, 2006). The prisoners faced something other than death: the radical conclusion of the liberal democratic ideal of transparency. Any privacy or veil of humility was stripped away from the prisoners, leaving them naked not only to the soldiers, but the global media. In the case of the prison, "It is really America that [...] electrocuted itself", unintentionally demonstrating the violence of their own liberal principles (Baudrillard, 2006). Both the free-flowing exchange of information and the liberal ideal of transparency revealed their horror in their own extension. The soldiers that performed the act, the media that exchanged the act, and even the television viewers who consumed the act, became principal actors in the war. Even those who consumed the act to criticize it paradoxically completed the violence, because the end goal of such a viral war was always to become globally exchanged and capture the minds of the viewer. Demonstrating Baudrillard's principal of reversibility, this act of horror returned humiliation upon the power that imposed it; a self-standing criticism of the entire apparatus of semiotic exchange. These unintentional instances of reversal demonstrate just how unstable power can until the semiotic exchange has reached its conclusion. Acts like these return a fatal criticism to every part of the process of symbolic exchange, regardless of the aggressor; "[...] those who live by the spectacle will die by the spectacle" (Baudrillard, 2006). Although media attention on cyber war lacks such grotesque images, like sexual degradation of the enemy, the function of information exchange remains militarized in a similar way. News coverage is not a representation of the war, but a manifestation of it. There is no distance to speak of, because the images are "[...] as virtual as the war itself, and for this reason their specific violence adds to the

specific violence of the war" (Baudrillard, 2006). Thus, the media representations of cyber war, like all modern conflicts, is destined to accumulate the obscene violence of global semiotic exchange in a way that is impossible to describe for many contemporary perspectives. It is not difficult to imagine a military hack which invades the privacy of an adversary's computer to symbolically eviscerate them, creating or revealing humiliating personal information while the media disseminates it across the globe. In that case, it is the digital body which is held under the microscope of transparency, because the real body is distanced from our perceptions in this war.

Media attention that warfare from a computer receives has no intention to display the potential brutality of response. There is no blood or gore in this conflict, and no geographical hot spot that can be pointed to. These characteristics reflect neither a cold war of pure deterrence nor a hot war of unmitigated destruction, but a kind of purgatory between the two. Although this phenomenon is not particularly new, considering that drone warfare has been prolific for quite some time, cyber war embodies the zenith of disassociating violence. Much like "the pilot in his simulator cockpit [...] surrounded by a virtual environment and motion-dependent images which are [...]" practically indistinguishable from an actual engagement, we grasp at straws for a distinction between the game and the event (Shapiro, 2014). In cyber war, the abstraction is even greater, with the enemy's water supply or electrical grid being represented as blips of code on a screen to be shutdown. The codes are infinitely circular representations of other codes, which are also simulations, and thus just as unreal as the battle itself. In the science fiction novel Ender's Game by Orson Scott Card, the protagonist performs simulated military exercises daily in preparation to command an offensive strike against the

opposing alien planet. The characters lack any knowledge of when, where, and if a war will happen, but they still train to command ships that are a lifetime away. Played like a virtual chess game, the military makes Ender's challenges progressively more difficult to prepare him for the day when he would assume command over the fleet. In the triumph of his final test, it is revealed to him that he just won the war, and the simulation technologies were simply a visual representation of what was actually being fought millions of light years away. There was a profound lack of reality in what was waged, and the victory celebrated on earth; the whole academy was an illusion that modeled a war of simulations. This example demonstrates the triumph of a simulated war, which is so far removed from any semblance of direct engagement that its relation to reality is practically indistinguishable. The teams at the school even participated in small skirmishes where they shot non-lethal weapons at each other in a battle room to train for the close quarters combat that we knew in retrospect would never come. This gave a "[...] dose of reality-effect [...]" to the participants, assuring them that a real shootingwar would indeed take place (Shapiro, 2014). Their role-playing shooter game was a mere facet of the whole simulation, decorating the game with antagonists and actual combat to maintain the integrity of the simulation. This is precisely what occurs in cyber war, "[...] the ghost-people must continue to exercise a certain 'minimal' function in the real" in order to preserve the supposed reality of the conflict (Shapiro, 2014). Games help to situate the conflict in reality, and the battles that can be tallied by the media work even better. Even when the media casts it in a negative light, a few blackouts or some victims of interference are ultimately necessary data points to keep the war intact.

The model of cyber war marks the disappearance of anything bodily, which fulfills a clean and purely operational type of war. "The victory of the model is more important than victory on the ground", writes Baudrillard, because war is now a "[...] strategy of relentless execution of a program" (Baudrillard, 1999). Yet this distance from the violence we enact generates a feeling that we have inoculated death in war, which is far from reality. When the enemy is an arrangement of code on a screen, this "produces 'a kind of isolation' from the violence of war that allows for its unrestrained prosecution" (qted. in Masters, 2010). This soldier has no relation to the reality of war; the devastation and lives lost to a power outage from a cyberattack would be entirely inconspicuous to their perception. The farther one treads from the terrain of the real, the more difficult it becomes to conceptualize those consequences in reality. Even the clinical language used by cybersecurity experts themselves illustrates a near-perfect level of compartmentalization. This is likened to the cold war where "[...] language was pitched at such a level of technocratic abstraction that it became almost impossible for those who employed it to grasp familiar notions such as war, death, or human destruction" (Debrix, 2001). Bombings became precision strikes, the ability to destructively incapacitate a nation with nuclear weapons became counterforce, and the murdering of civilian populations became collateral damage. The brutal subject of these terms are rendered abstract to our immediate perceptions and lose a key sense of reality. Yet there is an insidious balance that is struck in such word choices, because the propagation of threats from the media would not be persuasive if they did not appear somewhat spectacular. When Presidential Policy Directive 20 was officially rescinded in 2018, it gave the United States Department of Defense extreme latitude to offensively respond to cyber

threats however it deemed necessary (Johnson, 2018). The directive was sure to highlight potential threats to the United States, but the explanation of what Department of Defense action would look like was couched within an expert lexicon. Hack backs, internal active defense systems, and honeypots are just a few terms that offensive military action can often hide behind. The resulting bulwark between media and public perceptions allows the population to know the gist of the crisis without achieving true mastery of the technocratic language (Debrix, 2001). Like all twenty-first century conflict, this compounds the uncertainty of cyber war, which must remain foggy and driven by abstraction.

CYBER WAR AND THE EXTERMINATION OF EVENT

It is important to question what the end point of this supposed war is supposed to be. What seems to separate war from a slaughter or extermination is the struggle of somewhat evenly matched adversaries to contest control over territory or some material thing. If fighting for victory on the ground was the defining feature of many of the early wars of the 20th century, is it even possible to define the present global violence as war? This is not to insinuate a mere semantic distinction between the flexibility of executive waged conflict versus congressionally declared war, but something else entirely. Twentyfirst century warfare has been marked by the defeat of the more traditional notion of waras-fighting, ushering in the triumphant rise of non-war. Extreme instability and the propensity for a conflict to expand past the scope of anything demarcated in advance has vanished. There is a complete loss of event; Baudrillard argues that "anything that can occur must be predicted in advance, exterminated in advance" (qtd. in Bishop, 2009). War, which is executed as an omnipotent model, like discussed above, is a virtual affair that deters anything real from taking place. It can essentially be described as a "[...] deterrence of the real by the virtual" (Baudrillard, 1997). All that is left is a convincing screenplay of conflict that goes through the motions, desperate to convince the population of its own reality. "Film becomes war," argues Baudrillard "the two united by their shared overflowing of technology" (qtd. in Shapiro, 2014). In an entirely enclosed set, soldiers drop a few bombs for the cameras, fire shots for the reporters, and hack some

infrastructure for news websites. The extravagant set pieces show an eagerness to demonstrate the clear victory of one side but are eerily desperate to prove that there is indeed a war taking place. It is not an evenly matched duel with some amount of luck or spontaneous strategic thinking to determine the victor, but an entirely asymmetric affair; the more unequal, the more useful the film. Defeat of the model is never actually at stake; that would imply a lapse in control and the potentiality for an event to occur. Screenwriters for the global media apparatus nevertheless tease out the dramatic implications of military defeat, keeping the domestic population's eyes glued to the storyline on the screen.

For Baudrillard, this disappearance is not just of the physical referent, but also marks the symbolic disappearance of the body, leaving a void of subjectivity and social relations in the processing of war (Nordin & Öberg, 2014). There is a famous example he uses throughout his works from the novel *The Supermale* by Alfred Jarry to describe the vanishing limits between technological structuring and human beings. It depicts a 10,000-mile bicycle race between a five-man bicycle and a train. Together, the cyclist's function as a single machine to race the train, but in doing so lose their humanity along the way. One of the cyclists literally dies of exhaustion, yet his corpse keeps on riding to perform the task, which illustrates the bodies disappearing into the process itself (Nordin & Öberg, 2014). In Jarry's novel, the individual human, their particular characteristics, and their relation to anything except the repetitive completion of the process become irrelevant as they achieve machine-like synchronization. Cyber war interconnects with a plethora of military strategies to form a unified model capable of being consistently executed across all domains of combat without failure. Importantly, this achieves

complete asymmetry over the adversary, like a game tutorial that lays out a linear progression of moves for the player to achieve victory. The "[...] seamless economy of violence", Baudrillard argues, is "[...] a systemic violence which stems from the way in which war is operationalised" (Nordin & Öberg, 2014). Our focus on particular battles perhaps masks the more destructive nature of perfecting an obscenely specific model. In recent years the United States national security establishment has mapped and labeled the critical infrastructures of society – assets of the utmost importance that could potentially be threatened by a cyberattack (Smith, 2013). The role of military planners is then to repeatedly apply postures like 'defend forward' or the National Institute of Standards and Technology (NIST) framework to each sector. This is likened to an instruction manual for winning the cyber war, complete with an evolving checklist of actions that must be taken to defeat cyberterrorism in every area before it ever takes place. New symbols and steps to the model are consistently added, piling onto its excess of meaning and information, making the war more unreal. To be real there would have to be a potential for something new to happen, something that is not predicted, anticipated, and simulated from the outset by the model. Yet, as it is constantly shown on military newsletters, offensive and defensive postures around these checklists have become the principal mission of both the Cybercommand and Department of Homeland Security, who strive to perfect war by crossing off each step to completion. There is nothing spontaneous or reactive about the execution of this strategy, which would imply a lapse in the model's calculated control. This is where one can begin to see the horrendous violence of these omnipotent models. When there is no luck or desperation to speak of in war, it is akin to playing cards with a person who gets to know every move and card before it is played.

Despite military language of preemption creating global peace, abolishing mysteriousness does not end the violence of war, it allows one side to discover variance from the model and violently respond in anticipation of some terroristic act taking place (Bishop, 2009: 62). It seems the justification for all modern conflicts tend to follow this formula: create a blueprint (or simulation) of reality that ascribes global peace, amass intelligence (or information) to make that model become reality, and preemptively shutdown any event that may confound such a reality. This is precisely the pretense for the Iraq War "[...] whose aim was nominally the prevention in advance of Saddam's use of weapons of mass destruction" (Bishop, 2009: 62). The chance for the model of global non-proliferation to be violated became the justification for United States force, but even an invasion like this lacks any reality because it is also contained in the model. The complex diagrams of Afghanistan stability which went viral in 2010 absurdly listed every process necessary to win the war in immense detail (Nordin & Öberg, 2014). From the perspective, it is easy to see why a cyber war will never take place. Any supposed war will reiterate what has already been simulated or, with cyberweapons being increasingly categorized as weapons of mass destruction, be a banal rehash of a scripted preemptive war.

With the dominant execution of the virtual model leaving a ghost of what war used to be, it is no longer clear what is being fought over. In the new era of conflict, the real power does not lie within the strategic geopolitics of controlling territory. It is not the occupation of land or cities that is being threatened but, in a sense, occupation of the hearts and minds of billions across the globe. The new game of deterrence posits "[...] all of us as information hostages on the world media stage", and our fervent belief is the action which is threatened (Baudrillard, 1997). Models and simulations are destructive

insofar as our dedication and belief in them drives their violent imposition onto reality. This is a marked shift from the old deterrence regime, which was reliant on the virtual excess of destructive capabilities (Baudrillard, 1997). Instead, the exchange value is now the hostage, whose commitment to networking and consuming information must be won through media bombardment. It is not as if some god-like figure has structured the entire system of symbolic exchange, but rather it is a shared consequence "[...] to a will to information, to a will to meaning [...]" (Artrip & Debrix, 2014). Our desire to know everything about the war, to render every event meaningful, and to endlessly speculate over it manifests in mass global violence. In a sense, we are all simultaneously hostages to the global media apparatus while also being integral supporters of the violence it enacts.

The implications of what this means for the individual who consumes media to formulate a criticism of military action is perhaps where Baudrillard faces the staunchest academic opposition. It seems difficult to stand against military imperialism without being well informed about current events. Thus, it is frustrating to many academics who understand his critique to be "[...] passive indifference [...]" which would result in "[...] epistemic closure [...]" (Lovink, 2013). It is easy to see how nihilism or complete callousness to global violence could be interpreted from his texts. However, there is a high degree of nuance to Baudrillard's argument that makes it quite defensible. First, dissent is always accommodated in symbolic exchange because consuming the media's information, even when using it to criticize the war, is caught in the trap of affirming the war's reality. In fact, the public is exposed to this ineffective informative binary quite consistently; FOX News versus CNN, and Breitbart versus NBC demonstrate a few

polarizing examples. For Baudrillard, there would be no radical potential in affirming CNN's oppositional stance toward the conflict. To be for or against particular wars merely completes the great tautology, presupposing its own existence in the debate. This is sort of likened to the argumentative logical fallacy begging the question, which assumes the conclusion in its premises. When Baudrillard writes just prior to the invasion of Iraq, "[...] this war is a nonevent, and it is absurd to come to a conclusion about a nonevent", he is criticizing that type of self-positing certitude which refuses to question the reality of the event (Baudrillard, 2003). Second, such an oppositional stance is often just as complicit in global violence, like the aforementioned example in his essay War *Porn.* Viewing and publicly criticizing the images from the Abu Ghraib prison merely completed its violence because their potential to symbolically exterminate the prisoners were reliant on being globally viewed. Third, in less grotesque cases, amassing facts and information about the war, even when they are critical, simply contribute to the scope of military models. To expand these media representations of war, rendering what is unknown meaningful and visible, is to be complicit in the precoding of war. Asymmetric combat emerges from models with excessive information; producing new knowledge about the potential ramifications of the war would simply be integrated into the model, where a counterstrategy can be written in before the event takes place. As Baudrillard describes it, "we are not, however, in danger of lacking meaning; [...] we are gorged with meaning and it is killing us" (qted. in Artrip & Debrix, 2014). Who better to absolve the informative lapses in the model than the harshest critics of a conflict? Fourth, another perspective or piece of information about the war does not end the global violence, it amasses the oversaturated pile of information that is indifferently exchanged on a global

level. These images and representations of war are information, and information does not necessarily result in truth or certainty; it actually makes the event far less certain. For example, when CNN submits a claim about cyber war, it begets a counterclaim or response from FOX News and thousands of other media outlets. The result is not a clear and singular narrative, but an explosion of discourse that makes us less certain about any truth or validity and cyclically drives us to acquire even more information. Our end goal becomes entirely self-defeating because "information devours its own content", it is dissuasive instead of persuasive to the population (Baudrillard, 1981). It is not that knowing more about cyber war gets us any closer to penetrating the truth of the event, but instead locks us into the process of information searching, which is only a function of immersion in the virtual. Any contemporary mechanism of criticizing cyber war fails to plot a way out of its extensive violence.

TOWARD AN ILLUSORY READING OF CYBER WAR

If the core of global violence manifests from the accumulation of meaning, the only regress would be to abolish such a pursuit. Yet, our weapons to challenge this immense system of semiotic exchange are extremely limited since external critique, like described above, is increasingly coopted as an information commodity within the system (Pawlett, 2016: 33-34). Even the most radical intellectual theories that appear to be in diametric contradiction with the virtue of such exchange ultimately become tolerated and commodified. One can simply look at the plethora of radical critical literature books for sale on Amazon; purchasing copies of books like *The Communist Manifesto* "[...] not only provides profits to a tax-dodging mega-corporation, it also demonstrates (or rather, simulates) the openness, tolerance and freedoms of the consumer capitalist system" (Pawlett, 2016: 33-34). Thus, these oppositional challenges to commodification end up lauding the virtuous nature of commodification by proving a tolerance that is so complete that it can literally tolerate advocacies of its demise. Most criticism begins at the wrong place by placing their challenge in the domain of the real. For Baudrillard, an unreal system is incapable of receiving a real death and thus our strategy must be a weaponization of simulations that stage its symbolic downfall. This is why the previously mentioned principal of reversibility is of the utmost importance; even when one injects meaning that is toxic to the system's vitality, it will be consumed and exchanged like any other piece of information that is offered. Since the power of models that completely

envelope reality derives from their excess of information, the ability to know everything in advance, they are vulnerable to paradox and irreconcilable confusion. Over identification with the voracious consumption of information and the overproduction of meaning can therefore reverse its strength against itself, "[...] like a much larger opponent being thrown by the momentum of their own weight in martial arts" (Pawlett, 2016: 33-34). One can imagine, for example, a society taking the messages of Red Bull commercials far too seriously and consuming the beverage to the point of widespread intestinal dysfunction – a self-demonstrating critique of the culture of productivity.

As the entire system of symbolic exchange is a mere illusion, even a small act of deceit has the potential to cause its downfall. This is not to say that we should accelerate the proliferation of grotesque images like those of Abu Ghraib, quite the opposite, such a strategy would create obscene violence and fail to stake a true virtual challenge of the system. Rather, we should view those examples as demonstrations that even what initially appears impossible or destabilizing to exchange, will indeed be exchanged. Therefore, Baudrillard's solution is contained within the science of imaginary solutions coined as Pataphysics; "Pataphysicians fight reality [...]" not by confronting it, but by "[...] creating illusion and deceit" (Strehle, 2014). To avoid the trap of succumbing to a will to truth that landed us here in the first place, we must instead be radical enough to subvert reality by playing with simulations. Despite traditional assumptions, the purpose of radical thought should not be to "[...] recognize and analyze reality, instead it must deny and contradict its hegemony. It has to create illusion and establish a power of seduction that makes one lose the path of reality" (Strehle, 2014). This is comparable to a fishing lure, which takes advantage of the hunger and curiosity of fish to lead them astray from

their normal food course. Baudrillard's playful work mimics "[...] a simulacrum in the strongest sense" by denying seemingly obvious premises and writing in a riddle-like prose (Strehle, 2014). Language and signs are useful tools that can lead the subject to read and interrogate the event from a different angle. His propositions thus construct a new reality, and if the grand simulacrum is to oppose his illusion, it would expose its own unreality in the process. Yet critically, he is not concerned with discovering truth or crafting an evidence intensive case to create these illusions. By placing premises that contradict reality, his "[...] theories are like evil ghosts: They haunt reality by staging its excluded other—no matter if this other really exists or if it has to be feigned" (Strehle, 2014). This illusion of language attempts to replace what has been muted from the war by creating a new reality, not simply describing one that is waiting in the world. It replaces the old model with a confused and unreadable one in order to end the violence of predictability.

To disrupt the destructive communicative model of cyber war, we must build and weaponize radical simulations. Baudrillard coins this strategy as theoretical terrorism; it is likened to a graffiti artist who sprays their own meanings or words over the preexisting symbols on a building (Strehle, 2014). Suddenly, a new simulacrum disfigures and misguides the building's original connotation, imposing a code that is far less discernable than the last while laying a new reality over the old. Though we cannot spell out how this would exactly look for cyber war, as doing so would defeat the purpose of radical thought, we can be sure that it involves a shift in our model of communication. What is desperately needed is some way to pervert the supposed cleanliness of this cyber war, to confuse or distort its reality to the point of collapse. Much like how Baudrillard

responded to the Gulf War by completely withholding its dose of reality-effect, our antiwar stance could work over the cyber event, never opposing it on its terms. Without such a strategy, we are doomed to replicate the violence of simulations.

REFERENCES

- Artrip, R. E., & Debrix, F. (2014, May 1). The Digital Fog of War: Baudrillard and the Violence of Representation. Retrieved from https://vtechworks.lib.vt.edu/handle/10919/80496.
- Baudrillard, J. (2006). War Porn. Journal of Visual Culture, 5(1), 86–88. doi: 10.1177/147041290600500107
- Baudrillard, J. (2003, March 10). The Mask of War. Retrieved November 14, 2019, from http://www.ctheory.net/articles.aspx?id=494.
- Baudrillard, J. (1997). The Gulf War Did Not Take Place. Contemporary Sociology, 26(2), 138. doi: 10.2307/2076743
- Baudrillard, J. (1981). Simulacra and simulation. (S. F. Glaser, Trans.). Ann Arbor: University of Michigan Press.
- Bishop, R. (2009). Baudrillard now: current perspectives in Baudrillard studies. Cambridge: Polity.
- Cristiano, F. (2018). From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises. Journal of War & Culture Studies, 11(1), 22–37. doi: 10.1080/17526272.2017.1416761
- Debrix, F. (2001). Cyberterror and Media-Induced Fears: The Production of Emergency Culture. Strategies: Journal of Theory, Culture & Politics, 14(1), 149–168. doi: 10.1080/10402130120042415
- Johnson, D. B. (2018, September 21). White House touts new cyber strategy. Retrieved from https://washingtontechnology.com/articles/2018/09/21/wh-cyberpolicy.aspx.

- Lovink, G. (2013). After the Social Media Hype: Dealing with Information Overload. e-Flux, 45.
- Masters, C. (2010, May 20). Cyborg Soldiers and Militarised Masculinities. Retrieved from https://www.eurozine.com/cyborg-soldiers-and-militarised-masculinities/.
- Nakashima, E., & Warrick, J. (2012, June 2). Stuxnet was work of U.S. and Israeli experts, officials say. Retrieved November 12, 2019, from https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.
- Nordin, A. H. M., & Öberg, D. (2014). Targeting the Ontology of War: From Clausewitz to Baudrillard. Millennium: Journal of International Studies, 43(2), 392–410.
- Pawlett, W. (2016). Violence, Society and Radical Theory Bataille, Baudrillard and Contemporary Society. London: Taylor and Francis.
- Shapiro, A. (2014). Jean Baudrillard and Albert Camus on the Simulacrum of Taking a Stance on War. Retrieved November 12, 2019, from https://www2.ubishops.ca/baudrillardstudies/vol-11 2/v11-2-shapiro.html.
- Smith, S. L. (2013). Department of Defense Support to a Catastrophic Event. doi: 10.21236/ada589468
- Strehle, S. (2014). A Poetic Anthropology of War: Jean Baudrillard and the 1991 Gulf War. International Journal of Baudrillard Studies, 11(2). Retrieved from https://baudrillardstudies.ubishops.ca/a-poetic-anthropology-of-war-jean-baudrillard-and-the-1991-gulf-war/#5