THE DECONSTRUCTION OF NATION-STATE POWER AND THE MATERIALIZATION OF CYBER-STATES

Jonathan F. LANCELOT*

ORCID ID: https://orcid.org/0000-0003-0278-3419

Submitted: March 18th, 2019, Accepted: July 13th, 2020

Abstract

The focus of this inquiry is the prospect of the decline of nation-states and the emergence of cyber-states as governing institutions, resulting in a technological form of government that is automated, intelligent, and with minimum human intervention. The design of this paper will define the 'what is' and the nature of a cyber-state by *a posteriori* reasoning, uncovering the differentiated and empirical components we can observe, globalization and computer networks, cyberwarfare and autonomous weapons systems, e-governance, e-economy and virtual currency, and the internet as a new social contract. The decline of the nation-state is not a proposition of elimination; it is a suggestion of metamorphosis. The tradition of political philosophy is to ask the question, what is an ideal regime form? The streamlined nature of technology has swiftly integrated into the human condition to such a degree, political science as a discipline has struggled to incorporate the hard sciences fast enough to catch up with the development of cyberpolitics. The discipline of economics, however, has given the best foundation for empirical integration.

Key words: cyber-state, nation-state, cyberwarfare, e-governance, cyberpolitics.

What is a Cyber-State?

* A cyber security analyst at University of North Carolina Wilmington, and a principal policy analyst for the OSET Institute focused on election cybersecurity as a matter of national security. Jonathan graduated from Norwich University with a Master's in Diplomacy with a focus on cyber-diplomacy, and published the widely shared paper "Russia Today, Cyberterrorists Tomorrow: U.S. Failure to Prepare Democracy for Cyberspace," which is published in the Embry-Riddle Aeronautical University's *Journal of Digital Forensic, Security and Law*, and he is a contributor at *Small Wars Journal*. Mr. Lancelot is currently researching cyberpolitics, cyberphilosophy, cyberdefense, and the implicit bias in digital technology design and engineering of election administration technology. Jonathan is also a certified Apple computer administrator and has worked in the U.S. Senate and for the US Department of Defense.

I have thought it my duty to exhibit things as they are, not as they ought to be.

– Alexander Hamilton

A cyber-state or a cybercratic regime would be the proper successor to the nation-state within the social arrangement around cyberinfrastructure and social governance architecture. Cyber-states have not emerged in their complete form, yet the components of such leviathans have materialized in separate instances. Traditional nation-state governments have positioned themselves to rule over local, metropolitan, or wide area networks to set themselves up for metamorphosis with deliberate knowledge, or not, of the gradual process. For example, the only way nation-states can enforce their laws is through force of weaponry and coercion if the laws are not followed and broken. The way a cyber-state could enforce its laws is through code, data, and recorded instances in time, which can establish illegality by fiat, a form of enforcement. In other words, a surveillance state. This does not mean a cyber-state will not possess the forces of kinetic warfare or law enforcement, yet it would not be the sole means in displaying its power of enforcement upon citizens.

There are *a priori* yet disjointed components of the cyber-state that, when combined, articulates a complete system of government that could combine democratic, autocratic, or totalitarian aspects of traditional governance, yet with an extensive cyberinfrastructure of networked and collaborating automated systems. For example, the reduction of bureaucracy by replacing personnel with AI-driven decentralized autonomous organizations to restructure executive power. "Using algorithmic systems to manage an organization might sound almost like science fiction; however, over the past several years, experimentation with AI-based governance has already started" (De Filippi, Wright, 2018). The combination of these components can be induced *a posteriori* from pure reason. From an epistemological perspective, "there is an interesting connection between contemporary logical empiricism and classical rationalism that has not been sufficiently emphasized" (Rosen, 1960, p.453). Bridging the gap is essential in this exercise to separate the reality from the proposition yet add reality back into the proposition as an acceptable possibility. The opportunity to sequentially use philosophical observations first, then use pure reason is due to the confluence of computer science and philosophy, and second, the ancient relationship between philosophy and politics. "We have only just begun to see the influences of computer science on philosophy" (Hansson, 2008, p.477), especially in the realm of cybersecurity. Nevertheless,

we have only just begun to see the influence of computer science and cybersecurity on politics, and it requires political philosophy to deduce 'politics' down to its metaphysical source, the human. "What then is the impact of computing on people, and what should the proper political, social, and ethical applications of computing technology be" (Moor, Bynum, 2002, p.2)? For instance, the discipline of the ethics of cybersecurity is a useful tool for a philosopher to seek the truth on the matter. Logical reasoning will lead to the premise that a cyber-state can emerge to replace a nation-state as a means to govern, a logic that seems to baffle political scientists, whose methods of observation, experimentation, and conclusion have given doctrine to dangerous ideologies instead of intellectually decommissioning them. "Political theorists have failed to keep up with the times and have not engaged in sufficient value-free theoretical study of the raw data of politics, and partly that vast numbers of political scientists have falsely concluded that one of the important parts of the traditional study of political theory—political ethics—is not susceptible to scientific treatment and should be rigorously be eschewed" (Pennock, 1951, p.1081). Therefore, political philosophers have to lean on the discovery of international economists to begin to philosophize on the slow transformation in action. A cybercratic system reveals the accoutrements of a corporatist structure as private technology companies are innovating the technology instead of public institutions, placing implementation and administration of such governing systems in the hands of corporate entities instead of the public trust.

The Nation-State

There are numerous concepts and definitional conventions on what a nation-state is, and here we will set a clear definition of what it is. A nation-state is a combination of its people and its body of government. "In the language of classical metaphysics, the fatherland or the nation is the matter whereas the regime is the form" (Strauss, 1959, p.36) of the state. "The state is a body of government. "All the rules and laws, the government officials and their titles, the physical boundaries and those who define them –these make up the state" (Nation State: Definition, Examples & Characteristics, 2015). On the other side of the equation, there are citizens. "The nation is the people. The nation is created by a shared belief that the people inside a country are connected to each other" (Nation State: Definition, Examples & Characteristics, 2015). Both the nation and the state are held together by what Thomas Hobbes called a social contract, and what is commonly known as a constitution. "The

problem which Hobbes had to solve was concerning the relation between 'the mechanism of nature' and 'the social mechanism'. Man belongs to the natural mechanism and yet escapes it. Hobbesian man, through his nature, successfully revolts against it" (Berns, 1987, p.175). This revolution is a social contract between the people to establish a means and a form to rule themselves, escaping anarchy. The last trait that defines or is associated with the nation-state is nationalism, which is "a shared culture. This is often achieved through a common language, history, holidays, and education. Sometimes national culture is a result of similar people living in the same area" (Nation State: Definition, Examples & Characteristics, 2015). This can be taken further and stipulate that nationalism is a form of political ideology that feeds into the myth of the country's origin and a justification for the existence of the power of the ruling regime. Both the citizenry and the governing regime are both affected by the mutual human acceptance of computer network communication and technology. Nevertheless, we are focusing on the effect technology will have on governing regimes, and how nation-states could slowly evolve into cyber-states, where machines stand between the governed, and the regime.

Components of the Cyber-State

Nation-states, just as city-states, will be rendered weakened and feeble shadows of the powers they once were, and cyber-states are probable in superseding them. A cyber-state is a governing system that is automated, and the computerization of established practices like administration, legislation, central banking, and social services will be performed by artificial intelligence (AI), deep learning, blockchain technology, and networked systems at the most basic level. For instance, the role of administrator, bureaucrat, and politician can be semi- or fully autonomous depending on the configuration of the size, form, and agenda of governance. "The political content of many philosophical discussions still reflects terms of debate inherited from the industrial era and the rise of the nation-state" (Ronfeldt, 1991, p.65). Therefore, philosophy must revisit the metaphysics of politics in order to interpret cyberpolitics lucidly. The governance of cyber-states would be based on machine logic and deep learning AI along with human ideology and ambition, which formulates a new form of government, a cybercratic regime. The paper is designed to explain the 'what' is a cyber-state than the 'how' is a cyber-state; consequently all of the systematic features of a cyber-state

above will not be explicated here, as this is a broad stroke of a new look into the very ancient topic in political philosophy, the regime.

The first component is a historical and contemporary example, which is globalization and worldwide computer networks combined. James N. Rosenau states in his publication 'The Complexities and Contradictions of Globalization' defines globalization as "something that is changing human preoccupation with territoriality and the traditional arrangements of the state system" (Rosenau, 1997, p.363). In other words, state borders, law, culture, and economy are no longer a barrier to establishing institutional power over a region. It is the economic scientists who have written extensively on the question of the nation-state, yet schools of political scientists, not all, have struggled to reconcile with the phenomenon of nation-state decay. Susan Strange captures the essence of why the discipline of political science failed to integrate the science of economics properly. "Anyone who has been led by one path or another to the study of international political economy has probably shared the experience of being shot at from both sides—by the political scientists and by the economists. It feels as if one had been caught, defenceless and exposed, in the no man's land between two entrenched armies…against the political scientists, one is constantly crying for more attention to economic factors, to markets, to prices, to finance" (Strange, 1996, p.31). The quest for the manufacturing of ideological soldiers instead of skilled scientists has narrowed the discipline of politics into a risky academic venture, since business schools understand the power principles of globalization, and equip their graduates with a means to participate in the political power game at the highest levels. Globalization and computer networks both transcend nation-state borders; both are shared by citizens, consumers, and businesses with an interest in collective action to solve common issues, and this is understood by business schools intimately. In our search for the true nature of politics and the legitimacy of power, we must recognize "the sovereignty of the nation-state is in conflict with that of the megacorporate state" (Brinkman, Brinkman, 2008, p.427). When we add the proposition that the cyber-state will be the 'public' face of the megacorporate state, we can philosophically reason the existential subjection or end of nation-state dominance. In the realm of politics, computer networks and globalization facilitate the expansion of authority and interests of nonstate entities beyond existing territories and limits; in the realm of economics, both expand production, trade, and investments beyond local markets and economies, and both facilitate economic and technological innovation by transnational corporations (TNC). Political philosophical reasoning and empirical observation can deduce the possibility of tyranny by its

definition within this scheme of governance at the level of administration. However, "it is no accident that present-day political science has failed to grasp tyranny as what it really is" (Strauss, 1961, p.23). The reason for this failure to grasp this mode of governance is the confusion on contemporary power. "In contradistinction to classic tyranny, present-day tyranny has at its disposal 'technology' as well as 'ideologies'; more generally expressed, it presupposes the existence of 'science,' i.e., of a particular interpretation, or kind, of science" (Strauss, 1959, p.23). In other words, the expansion of technology into the realm of governing human society replaces political science with the rule of actual science. More specifically, the authority of nation-states over international and local economies have been compromised by design. Yet, "political science is haunted by the belief that 'value judgements' are inadmissible in scientific considerations, and to call a regime tyrannical clearly amounts to pronouncing a 'value judgement'" (Strauss, 1959, p.23). This assertion of 'value judgements' could not be further from the political truth on identifying possible regime forms at their most basic platform, as regimes affect the human senses and condition of being, the core by which humans articulate the value of their governing structure.

Technological innovations have economically empowered Silicon Valley companies as nation-states have weakened themselves with international austerity and deregulation policies. "In the minds of many Silicon Valley power players, the best thing that the federal government can do is leave them alone" (Lee, 2018, p.64). Nonetheless, this works towards the demise of the form of governance called democracy, and the demise of the guarantee of human rights if democratic regimes allow corporations to control the terms of governance. Corporations are not designed to confer alienable rights by positive legalism, and they will not. It is the national policies of nation-states that guarantee their citizens the right to participate in governance and guarantee the human rights of the citizen, at least the right to not be controlled at a sufferable degree, if the regime is a democracy. Globalization, producing an active and profitable international market for private powers, the very definition of tyranny, has set the foundation for the emergence of cyber-states. The idea of the cyber-state itself is not tyrannical; it is the foundation that a cyber-state is built upon, which is unquestionably undemocratic.

The second component of a cybercratic regime is cyberwarfare and autonomous weapons systems. Semiautonomous weapons systems are engaged when a human in the loop decides which target is the objective. Supervised autonomous weapons systems can search, detect, decide to target and engage targets on their own, yet a human can interfere and change the decision made by the system. Fully-autonomous weapon systems are when humans are completely out of the loop, and AI and machine learning is employed. Is automated warfare a path towards the best way of life? When philosophers question what the best way of life is, or the best life, we must ask of ourselves is the life we are living as citizens a just life? If we turn to the ancient city-state of Athens during the Peloponnesian War through Thucydides, we will see a society consumed by what they understood was a just life. "Men disregarded the apparent restraining power of law or justice even when such behaviour served no interest of their own, except perhaps to satisfy an immediate passion" (Bolotin, 1987, p.16). It is this collective delusion of glory and the acquisition of gaining an empire, which would lead to a 'just' way of life that was a factor that led to deadly war. Athens fell in and around 404 B.C.E., and every major war in history had the element of 'glory for the acquisition of an empire' within its formula.

The integration of AI and weapons of war by the military technological complex is for glory, passion, and what is perceived as the best life. Presently, war is a permanent and continuous asymmetrical state of violence, free of the control of any traditional body politic, least of all, any attempt of control over violence by such institutions increases the likelihood of maintaining the uninterrupted motion of extreme death. "We know, certainly, that war is only called forth through the political intercourse of government and nations; but in general it is supposed that such intercourse is broken off by war, and that a totally different state of things ensues, subject to no laws but its own" (Clausewitz, 1832, p.698). The more modern the war in history, the deadlier it is. Integrating the use of technology into the wars of men have always been progressively problematic for the survival of the human race over the course of history, from the Peloponnesian War to the Atomic Age. Carl Von Clausewitz axiomatically linked politics as being existentially attached to war. In reality, politics is the beginning and the end of human society, war at one end, and peace on the other. We must deductively conclude that some who are among those who live a political life believe war to be the means towards the best life, which is to rule a hegemonic power under their ideological image, just as the Greeks, the Romans, and the French under Napoleon attempted to do historically,

which eventually failed to secure peace. In other words, realism advises us that those within the political life who believe war will lead to the best life will be met with disaster.

Therefore, how do cyberpolitics and cyberwarfare relate to this, and differ? The relation of traditional politics and cyberpolitics dwells within the limits of the human experience or the human condition. Every human being is responsible for politics, within or without an explicit social contract. Politics is built into the ontological nature of a human being, whose will to survive could take the form of peace or war. "Hence the social mechanism is as natural as the natural mechanism. The social mechanism is a prolongation of the natural mechanism: the continuity of the natural and the social mechanism is in no way broken" (Berns, 1987, p.175). Cyberpolitics is the delineation of this natural state of human integration within the fifth domain, beyond the limits of the discipline of political science. This leads to the difference between traditional politics and cyberpolitics.

Political scientists serve a purpose, yet the ideological lenses of their teachings distort the view of economics and war. Cyberpolitics could very well stand on its own as a scientific and technical practice of politics that is best understood in terms of political philosophy, cybersecurity, and computer science. In other words, cyberpolitics functions outside the ideological teachings of political science. Case and point, the discipline of political science "includes eight distinct theories of international relations, with two positions being divided across classical and neo-variants: realism/structural realism, liberalism/neoliberalism, the English School, constructivism, Marxism, critical theory, feminism, poststructuralism, green theory, and postcolonialism" (Dunne, Kurki, Smith, 2016, p.3).

Political Science is a discipline that is going in many opposing and contradictory directions, which is confusing for all who are attempting to educate themselves on how to avoid the least favourable means to rule, be ruled, and wage war.

Traditional Warfare relates to cyberwarfare as it is an expansion of defensive and offensive capabilities of not only military organizations, non-state organizations have expanded capabilities within the same space as nation-state actors. Depending on the technology that is

implemented in the act of violence, such as drone warfare, incendiary devices, or cyberattacks, nation-state military organizations maintain dominance within the field of battle, yet this dominance is questionable in cyberspace.

The difference between traditional warfare and cyberwarfare is the prospect of humans handing over the responsibility of violence to AI, where the weapon makes the decision where to strike, who, and when. Undeniably, war has always been within the existential domain of humanity, whether there was a lack of ethics and law, or full adherence to the laws of war. The traditional question of ethics is "can nations be morally responsible for the wars they are involved in, or should only those with the power to declare war be held responsible" (www.iep.utm.edu/war/)? Cyberwarfare begs another question, can a nation, the state, or the tech company be morally responsible for the wars that involve weapons that think and make decisions for themselves without a human in the loop? This sort of warfare is possible on all fronts, land, sea, air, space, and of course, cyber. If machines are sent to destroy human beings in war, can we define this as war, or is it mass murder or genocide? "The morality of war traipses into the related area of political philosophy in which conceptions of political responsibility and sovereignty, as well as notions of collective identity and individuality, should be acknowledged and investigated" (www.iep.utm.edu/war/).

Political scientists seem to have failed at the task of anticipating the effect computer science would have on war, or that governments in realpolitik would actively ignore or conceal the implication of automated war. This would be the most dangerous component of a cybercratic regime.

The third component is Estonia's innovation of e-governance, and it is a central component of a cyber-state, as it is a civic function, and in Estonia's case, democratic in nature. Estonia maintains a government cloud service that converts public services into adaptable e-solutions for its citizens and e-residents. Democratic processes of voting are included, designed to help citizens stay engaged in the process of governance. e-Cabinet is an authoritative apparatus that the Estonian government use to streamline its decision-making process. Lastly, Data Embassy allows for the state to continue operating under conditions where local data centres

are compromised. Cybersecurity and blockchain technologies are implemented for accountability and risk management within the system. Nevertheless, in all of this advancement in technological governance, a philosophical question should ask, can the government prove that this cybercratic infrastructure that supports the democratic regime will not, in turn, support a totalitarian regime? This is not questioning the integrity of Estonia's political culture; this is a question based on Plato's observation of democracy in *The Republic*. It is not beyond reason to question the power of trust when compared to the totalitarian tendencies of political ideology and the power of ideologues within democracies to get elected. "It would be wrong to assume Estonia is a depoliticized nation, standing apart from trends that other liberal democracies are witnessing" (Berson, 2018), a rise in ideological populism. Dr Viljar Veebel supports this assumption when he states "for nearly two decades, a liberal social consensus existed: with each year of independence, Estonians expected that their civil society and democratic institutions would grow ever stronger. Then, an unexpected change occurred in 2014-15 fracturing this flawless image. A previously marginal anti-European populist party, the Conservative People's Party of Estonia (EKRE), started gaining popularity…there are many reasons for this dramatic rise.

First, a wider social dissatisfaction with the policies of previous coalition parties that had become more and more blind or ineffective toward some social problems (inward and outward mitigation, sovereignty, and economic sustainability) or groups (farmers, people with lower income, etc) took root" (Veebel, 2019). In Plato's Republic, Socrates clarifies democracy susceptibility to becoming a tyranny by stating "shall we definitely assert, then, that such a man is to be ranged with democracy and would properly be designated as democratic? Moreover, now the fairest polity and the fairest man remain for us to describe, the tyranny and the tyrant. Come then, tell me, dear friend, how tyranny arise? That it is an outgrowth of democracy is fairly plain" (Plato, 1961, p.790). Estonia ought to oversee the changes with exceptional care for the *dêmos*. To quote Leo Strauss again on the atomism of the nation-state, "the fatherland or the nation is the matter whereas the regime is the form" (Strauss, 1959, p.36). The matter is the foundation of the form, and without matter, the form is assumed to be the matter.

All democracies must be mindful of its matter; otherwise the form of tyranny assumes power. In this case, we must question the use of e-governance in the hands of those who would use democratic means towards ideological and totalitarian ends. One of the best analogies that one could contemplate is the technology of the rocket, which can be used as a means for exploration, or as a weapon of mass destruction. If we are all compelled towards cyberspace, which serves as our new social contract by fiat, and a means toward our new social order where we collectively choose to subject our personal data to be protected and managed by experts, can we trust that democracy or more so, a digital democracy will not deliver itself as a totalitarian regime? In other words, the difficulty is not technology; it is the political animal indoctrinated with ideology and an appetite for power that is problematic. Tyranny is in the human, and totalitarianism is the use of technology by the tyrant.

The fourth components of a cyber-state are the e-economy and virtual currency (VC). VC instruments would be the central feature of a cyber-state, just as a traditional economy is central to the existence of the nation-state as a source of power and is at the core of the proposition that nation-states will eventually become an obsolete mode to governance. Money or currency was defined by Karl Marx's in Das Kapital as "the chief function to supply commodities with the material for the expression of their values, or to represent their values, or to represent their values as magnitudes of the same denomination, qualitatively equal and quantitatively comparable" (Marx, 2009, p.55). Today, we use fiat currency that is backed by the government that issues them instead of a commodity and supported by supply and demand, and the stability of the issuing government institution.

The possibility of the existence of fiat currency was stated by Marx that "since the expression of the value of commodities in gold is a merely ideal act, we may use for this purpose imaginary or ideal money" (Marx, 2009, p.56). Most importantly of all, "money itself has no price" (Marx, 2009, p.56). L. Randell Wray expanded on this description on the 'thing' called money affirming "our system (the United States) is a state money system. Our currency is government's liability, an IOU that is redeemable for tax obligations and other payments to the state. The phrase 'debt-free money' is based on a non-sequitur or misunderstanding. Remember, anyone can create money, the problem is getting it accepted" (Wray, 2015, p.7). This is why the VC Bitcoin was an explosive revolutionary instrument that brought the

weakness of the nation-state fiat currency system into scrutiny. The foundation of nation-states power is its economic engine. Nevertheless, the power of money requires trust and faith from those who use the currency. “Aristotle outlined four properties that constituted good money.

First, the currency must be durable, and not waste away through the ravages of time. Next, it should be portable, so that traders can easily bring money wherever they wish to exchange value. Third, it should be divisible, to allow more precise exchanges of value for like value. Finally, it must have some kind of ‘intrinsic value’, increasing what the economist Carl Menger called the ‘saleableness’ of money” (O’Sullivan, 2018, p.93). Bitcoin possesses all of these qualities. Given the nature of computer technology, and the ability to continuously update open-source software and network capability, Bitcoin is assumed to pass all of Aristotle's requirements. In other words, Bitcoin has demonstrated that VCs can, in fact, exist beyond the reach of nation-state power and can be used as a means to evolve the governance of economy or replace the traditional means to control the economy.

The technology is contemporaneous. “Some commentators argue that Bitcoin may, in the long run, replace the US dollar as the world’s reserve currency. They maintain that continued financial crises wrought by the mismanagement of global currencies will, over time, increase the exodus to Bitcoin as a stable store of value. If this state of affairs came to pass, it would represent a virtual coup in the state of global power dynamics” (O’Sullivan, 2018, p.93). There is a potential for the collapse of economies and societies of weaker nation-states, and three possibilities emerge from empirical deduction: the initiation of weaker nation-states, the occurrence of persistent failed states, or the materialization of cyber-states.

The last component that will be enumerated here is the new social contract. Currently, humanity has agreed to a new social contract, not out of what Thomas Hobbes coined "continual fear and danger of violent death, and the life of man, solitary, poor, nasty, brutish, and short" (Hobbes, 1984, p.76), humanity joined this social contract because of the fear of missing out and being left behind. The new social contract is the internet, or what we nowadays call cyberspace. Terms of agreements are approved by those who want to connect

with others through their computers, smartphones, and the internet-of-things (IoT), setting into question the future of old social contracts and ancient modes of being governed. Humanity is stepping out of the protection of sovereign order into a state of nature in cyberspace, which manifests in the physical world as anarchy and lawlessness. The main variance between the proposition and Hobbes' theory is the unconscious agreement to the social contract (which is humanity saying we want to become an ordered society in this manner) that happens to be a constitution of hardware, firmware, and software linked together by communications networks forming nodes of communications internationally. It does not readily produce a sovereign or social order. The reason why is the sovereign produced by this sort of social contract is not a Westphalian nation-state as its mode of sovereignty is ill-structured and antiquated.

The social contract of cyberspace challenges traditional sovereign nation-states, as the new social contract is tangible and networked by hardware, firmware, and software. Traditional social contracts, which creates positive laws for the people to follow, are mere abstractions that even governmental regimes circumvent and violate in order to seize more power. Now individuals, including corporations, have the means to circumvent sovereignty. Is Hobbes sovereign leviathan dead, or has it transformed, or is it being replaced? It has transformed. If we are all compelled towards the governance of a cyber-state, whose power is defined by a new social contract, and a means toward our new social order where we collectively choose to subject our personal data to be protected and managed by cybercratic administrators, can we trust that this system of governance will not deliver itself as a totalitarian regime? In other words, the difficulty is not trusting one's life to technology, that is elementary. The difficultly occurs when that trust is abused.

Conclusion: A Defence of Reasoning

Plato's Republic was the beginning of political philosophy's question of what the best regime is, and which form of government is preferable to justice, if one can find an adequate definition of what justice is. One could say justice is a derivative of reprisal, or "justice is everyone minding their own business" (Stevens, 2011, p.126), yet a regime is designed and

sometimes an imposter towards what a nation or a people define as what justice is. Socrates and the interlocutors first attempt to define justice, then proceeded to philosophize an ideal state into metaphysical existence *a posteriori*. Out of pure reasoning, they extracted the basic principles of a just government. "The law is not concerned with the special happiness of any class in the state, but is trying to produce this condition in the city as a whole, harmonizing and adapting the citizens to one another by persuasion and compulsion, and requiring them to impart to one another any benefit which they are severally able to bestow upon the community, and that it itself creates such men in the state, not that it may allow each to take what course pleases him, but with a view to using them for the binding together of the commonwealth" (Plato, 1961, p.752). Henceforth, this philosophical inquiry is an introductory attempt in following the tradition of political philosophy by using empirical elements a priori to bring into reason an ideal state. In the case of the proposition of the cyber-state, what is brought into reason is not so much an ideal state as it is a probable state. Aristotle confirms this approach by stating "as in other departments of science, so in politics, the compound should always be resolved into the simple elements of least parts of the whole, we must therefore look at the elements of which the state is composed, in order that we may see in what the different kinds of rule differ from one another, and whether any scientific result can be attained about each one of them" (Aristotle, 1952, p.445). The main element we are focused on as a catalyst to the fundamental change to governance is computer science, which within the observation of the merging of politics and technology has indeed marked the beginning of politics as a science.

Some counterarguments can be directed towards the proposition of this paper; two will be explored. First, the crucial concept is the nation, the other half of nation-state, which could serve as a problem to the idea of a cyber-state. One could counter the proposition of cyber-states emerging from the demise of nation-states by stating the nation is a collective state of being that is psychological, where yes, the perception of justice is approximately in common, and there is an approximation of a common culture and norms. A nationality is a common approximation of an understanding of peoplehood that has linguistical implications within a regional vernacular. For example, British, American, Ethiopian, and Chinese. The nation is a constant that is dependent on the immovability of a generational inheritance of identity. The state or the regime is a manifestation of the will of the nation or could potentially be. A cyber-state would be a new and improved nation-state, a nation-state, nonetheless.

Naturally, this argument on the nation would be a valid rebuttal to the proposition of this philosophical inquiry, especially if we consider that a nation is a collective identity with psychological and sociological implications. Conversely, this counterargument would illuminate a fact that would be immaterial to the *a posteriori* reasoning of the cyber-state. Cyberspace already overlaps national borders, cultures, languages, norms, notions of justice, and perceptions of the best form of government. The focus of this paper was on the nature of technology on the regime, and not so much the nation. Yet, it could be stated that cyberspace is already eroding psychological foundations of national identity, and worth a deep philosophical inquiry on its own as the complexity of the human relationship with society and authority is considerable.

The next argument against the emergence of cyber-state power is the enforcement power of nation-state military and police organizations, as they are the arm of enforcing the laws of the nation-state and preventing the demise of the Westphalian order. Military and police organizations are creatures of the law and a full expression of state power. They are usually written into a social contract or constitutional agreement, and subject to legislative, judicial, and executive departments of a governing structure. "Is not war merely another kind of writing and language for political thoughts" (Clausewitz, 1832, p.699)?

Military forces throughout history have been more technologically advanced than the civilian segment of a governing regime, and today more technologically advanced than domestic police forces. If citizens are in the mode of revolt, the domestic police are the enforcement arm of the regime to push back on revolution against the state. Just the same, if a cybercratic revolution tried to override the sovereignty of the law, legislation, and executive power over the people, military or police forces would protect traditional government structures and social contracts by staying loyal to the traditional nation-state form, keeping the process of traditional law-making safe from innovation and the misplacement of power. In other words, protecting the lawyers.

There is no argument that military and police organizations are creatures of the law and the full expression of state power. Nevertheless, a corporation is also a creature of the state, yet are corporations beholden or subject to the governing power of the state? We can comfortably determine that it is questionable. “We have to rethink some of the assumptions of conventional social science” (Strauss, 1961, p.4), especially when power and ethics is a concern. The debatable nature of the relationship between the state and the corporation ought to apply to military and police organizations in turn. Consequently, who has more power, the soldier or the lawyer? Why do some generals follow the law, and others break the law? Why do some police officers enforce the law, and others go beyond it? Why do some corporate executives adhere to the law, and others believe the laws do not apply to them? These questions go to the core of how much independence these organizations and their functionaries possess against the laws of the state. Absolute loyalty to the traditional means to realize positivism and defining by traditional means what positive law and legal institutions are is a weak defence against the prospect of a cybercratic revolution. In other words, military, police, and corporate power can be redirected away from positivist legal institutions, or the public institutions that created them in the first place. Legal institutions with lawyers and politicians alone yield no power without the enforcement and monetary power of the above, even if the state has the power to control the creation of monetary instruments.

The foundation of the philosophical proposition of a cyber-state, in relation to the study of globalization, can be found within the research of economic schools, specifically the work of economists Susan Strange, Richard L. Brinkman, and June E. Brinkman. Obviously, philosophy ought not to defend itself as it has the capacity to seek how deep politics is within the ontology of human experience, yet a defence of what is proposed for further philosophical study is warranted, and obligatory. International economists have noticed that "nation-state sovereignty, while not dead, is currently in decline" (Brinkman, Brinkman, 2008, p.429). When establishing the technology as a means toward governing, Brinkman found “a given structure of technology does not necessarily provide a basis for evaluation. Evaluation rests upon what is done with the structure, which in turn, is predicated upon human behaviour and that behaviour, in turn, rests upon a process of institutionalization” (Brinkman, Brinkman, 2008, p.427). To assume the implementation of technology to rule or to continue with the

same form of governance, or be a champion for the propagation of democracy, or become a significant tool for totalitarianism is not looking at the truth of politics.

In comparison to the ancient technology, “the nation-state is neutral, as a polity of governance, in terms of evaluation” (Brinkman, Brinkman, 2008, p.428). It is within the context of knowing the truth of what politics is, and how an individual or society views the experience of politics and its doings is what determines the orientation of rulers. Nevertheless, technology itself, by its deterministic nature, can become a tool for tyranny than for democracy if there is a presumption of the strength of convention to resist injustice, or a justice that is opposite of the norms of a democratic society. "Will cybercratic regimes favour democratic or authoritarian and totalitarian tendencies? At present the information revolution seems to strengthen democratic forces around the world. Nevertheless, totalitarian cybercratic regimes also remain a possibility” (Ronfeldt, 1991, p.55). Democratic nation-states ought not to rest on their political moralities alone.

It is contemporary political science that is in need of a defence, not political philosophy. It is the discipline of international economics that provides a foundation for contemporary political philosophers and computer scientists to intellectually collaborate on politics and the forms of governance to emerge from integration. “It is not uncommon nowadays to find philosophers and computer scientists forming teams to explore intellectual subjects common to philosophy and computing” (Moor, Bynum, 2002, p.3). As established before by Susan Strange, contemporary political scientists have dug themselves into a trench, where it opposes international economics. We can deduce that those trenches are also designed to keep philosophers and computer scientists from spotting their weak claims to science or truth on political things. “Another way of putting this is that science is more than just the collection of facts or specimens: science is about solving puzzles. A puzzle is a problem or group of related problems which does not have an obvious solution. To solve a puzzle, you have to observe the facts closely, decide which facts are relevant and which are not, making imaginative guesses, and then check your guesses using rigorous logical reasoning” (Salkie, 1990, p.13-14).

Ideology, which is the problem of political understanding with roots in political education, is not a science. In closing, the proposition of this inquiry deals with the 'what' is a cyber-state than the 'how', 'who', 'where', and 'when' is a cyber-state. Even with the attempt to pull the star prematurely over the horizon, this introductory exploration has failed to capture the full spectrum of a fully materialized cyber-state. For example, extensive discussions were deliberately excluded on blockchain technology, AI, and IoT, which would be extensive papers on the same subject matter in themselves. What was most important in this exercise was the attempt to estimate by logical reasoning a potential regime structure by separate and functioning empirical components. The abuse of power using technology can be reasonably proven, and this is why the profession of cybersecurity exist, yet even cybersecurity could be abused depending on politics. Hence, politics itself must be meticulously re-examined, dissected, and reintroduced into the sciences.

References

Aristotle. (1952). Politics. London: Encyclopedia Britannica, Inc.

Brinkman, R, and Brinkman, J. (2008). Globalization and the Nation-State: Dead or Alive. Journal of Economic Issues 42, no. 2: 425-433.

Cropsey, J, and Strauss, L. (1981). History of Political Philosophy. Chicago: University of Chicago Press.

De Filippi, P., Wright, A. (2018). Blockchain and the Law: The Rule of Code. London: Harvard University Press.

Dunne, T, Kurki, M, Smith, S. (2007). International Relations Theories. Oxford, UK: Oxford University Press, USA.

e-Estonia: the ultimate digital democracy? (2018) Medium Blog, November 4, 2018.

Hansson, O. (2008). Philosophy and Other Disciplines, Metaphilosophy 39, no. 4/5: 472-483.

Hobbes, T. (1994). Leviathan. Cambridge, UK: Hackett Publishing.

Lee, K. (2018). AI Superpowers: China, Silicon Valley, and the New World Order. : Houghton Mifflin Harcourt.

Marx, K. (1996). Das Kapital. Washington DC: Regnery Publishing.

Moor, J, and Bynum, T. (2002). CyberPhilosophy. : Wiley-Blackwell.

Moseley, A. (2020). War, The Philosophy of | Internet Encyclopedia of Philosophy: https://www.iep.utm.edu/war/.

Nation State: Definition, Examples & Characteristics - Video & Lesson Transcript | Study.com." Accessed May 2020. https://study.com/academy/lesson/nation-state-definition-examples-characteristics.html.

O'Sullivan, A. (2018). Ungoverned or Anti-Governance? How Bitcoin Threatens the Future of Western Institutions. Journal of International Affairs Editorial Board 71, no. 2: 90-102.

Randall, L. (2015). Modern Money Theory. New York, NY: Palgrave Macmillan.

Roland Pennock, J. (1951). Political Science and Political Philosophy. The American Political Science Review 45, no. 4: 1081-1085.

Ronfeldt, D. (1991). Cyberocracy, Cyberspace, and Cyberology: Political Effects of the Information Revolution. RAND Corporation.

Rosen, S. (1960). Political Philosophy and Epistemology. International Phenomenological Society 20, no. 4, 453-468.

Rosenau, J, N. (1997).The complexities and contradictions of globalization. *Current History* 96, no. 613 (1997): 360.

Salkie, R. (1990). The Chomsky Update. Boston: Unwin Hyman.

Stevens, R. (2011). Political Philosophy. New York, NY: Cambridge University Press.

Strange, S. (1996). The Retreat of the State. Cambridge, UK: Cambridge University Press.

Strauss, L. (1988). What is Political Philosophy? And Other Studies. Chicago, Il: University of Chicago Press.

Strauss, L. (1991). On Tyranny. Chicago: University of Chicago Press.

The Collected Dialogues of Plato (1961). Princeton University Press.

Veebel, V, (2019). The Rise of Right-Wing Populists in Estonia - Foreign Policy Research Institute. Accessed May 31, 2020. https://www.fpri.org/article/2019/07/the-rise-of-right-wing-populists-in-estonia/.

Von Clausewitz, C. (2004). On War. New York, NY: Barnes & Noble Publishing.