## T

#### Interpretation: The affirmative must be topical.

#### “Resolved” denotes a formal resolution.

**AWS ’13** [Army Writing Style; August 24th; Online resource dedicated to all major writing requirements in the Army; Army Writing Style, "Punctuation — The Colon and Semicolon," <https://armywritingstyle.com/punctuation-the-colon-and-semicolon/>]

The colon introduces the following:

a.  A list, but only after "as follows," "the following," or a noun for which the list is an appositive: Each scout will carry the following: (colon) meals for three days, a survival knife, and his sleeping bag. The company had four new officers: (colon) Bill Smith, Frank Tucker, Peter Fillmore, and Oliver Lewis.

b.  A long quotation (one or more paragraphs): In The Killer Angels Michael Shaara wrote: (colon) You may find it a different story from the one you learned in school. There have been many versions of that battle [Gettysburg] and that war [the Civil War]. (The quote continues for two more paragraphs.)

c.  A formal quotation or question: The President declared: (colon) "The only thing we have to fear is fear itself." The question is: (colon) what can we do about it?

d.  A second independent clause which explains the first: Potter's motive is clear: (colon) he wants the assignment.

e.  After the introduction of a business letter: Dear Sirs: (colon) Dear Madam: (colon) f.  The details following an announcement For sale: (colon) large lakeside cabin with dock

g.  A formal resolution, after the word "resolved:". Resolved: (colon) That this council petition the mayor.

#### “The member nations of the World Trade Organization” are 164 governments loosely tied by commitment to global trade

CalChamber ND, The CalChamber, in keeping with long-standing policy, enthusiastically supports free trade worldwide, expansion of international trade and investment, fair and equitable market access for California products abroad and elimination of disincentives that impede the international competitiveness of California business. Likely post-2020. “World Trade Organization” <https://advocacy.calchamber.com/international/trade/world-trade-organization/> brett

The WTO and its 164 member nations is the only global international organization dealing with the rules of trade between nations. At its heart are the WTO agreements, negotiated and signed by the bulk of the world’s trading nations and ratified or approved in their parliaments or legislatures. The goal is to help producers of goods and services, exporters and importers conduct their business.

#### “Reduce” means diminish.

Friedman ’99 [Daniel; February 9th; Senior Circuit Judge; Cuna Mutual Life Insurance Company, “Plaintiff-Appellant, v. UNITED STATES,” https://cite.case.law/f3d/169/737/615055/]

"The amount determined" under § 809, by which the policyholder dividend deduction is to be "reduced," is the "excess" specified in § 809(c)(1). Like the word "excess," the word "reduced" is a common, unambiguous, non-technical term that is given its ordinary meaning. See San Joaquin Fruit & Inv. Co., 297 U.S. at 499. "Reduce" means "to diminish in size, amount, extent, or number." Webster's Third International Dictionary 1905. Under CUNA's interpretation of "excess" in § 809(c), however, the result of the "amount determination" under § 809 would be not to reduce the policyholder dividends deduction, but to increase it. This would directly contradict the explicit instruction in § 808(c)(2) that the deduction "be reduced." The word "reduce" cannot be interpreted, as CUNA would treat it, to mean "increase."

#### “Intellectual property protections” are legally established rights

Trevor Brewer 19, legal advisor @ BrewerLong Business Law, “WHAT ARE THE FOUR BASIC TYPES OF INTELLECTUAL PROPERTY RIGHTS?” <https://brewerlong.com/information/business-law/four-types-of-intellectual-property/> brett

When a business or an individual has an idea that they want to protect from being used by others without their permission, it is best to seek legal protection of that intellectual property.

By seeking property rights over your intellectual property — property that is a creation of the mind, such as an invention, symbol, or even a name.

You establish rightful ownership and prevent the unlawful use of your property.

What’s more, establishing intellectual property rights can help to fuel the economy and stimulate further innovation.

There are four main types of intellectual property protections, reviewed below. Work with an experienced intellectual property attorney to learn more about steps to take to secure the necessary protection for your intellectual property.

FOUR TYPES OF INTELLECTUAL PROPERTY PROTECTIONS

There are four types of intellectual property rights and protections (although multiple types of intellectual property itself). Securing the correct protection for your property is important, which is why consulting with a lawyer is a must. The four categories of intellectual property protections include:

TRADE SECRETS

Trade secrets refer to specific, private information that is important to a business because it gives the business a competitive advantage in its marketplace. If a trade secret is acquired by another company, it could harm the original holder.

Examples of trade secrets include recipes for certain foods and beverages (like Mrs. Fields’ cookies or Sprite), new inventions, software, processes, and even different marketing strategies.

When a person or business holds a trade secret protection, others cannot copy or steal the idea. In order to establish information as a “trade secret,” and to incur the legal protections associated with trade secrets, businesses must actively behave in a manner that demonstrates their desire to protect the information.

Trade secrets are protected without official registration; however, an owner of a trade secret whose rights are breached–i.e. someone steals their trade secret–may ask a court to ask against that individual and prevent them from using the trade secret.

PATENTS

As defined by the U.S. Patent and Trademark Office (USPTO), a patent is a type of limited-duration protection that can be used to protect inventions (or discoveries) that are new, non-obvious, and useful, such a new process, machine, article of manufacture, or composition of matter.

When a property owner holds a patent, others are prevented, under law, from offering for sale, making, or using the product.

COPYRIGHTS

Copyrights and patents are not the same things, although they are often confused. A copyright is a type of intellectual property protection that protects original works of authorship, which might include literary works, music, art, and more. Today, copyrights also protect computer software and architecture.

Copyright protections are automatic; once you create something, it is yours. However, if your rights under copyright protections are infringed and you wish to file a lawsuit, then registration of your copyright will be necessary.

TRADEMARKS

Finally, the fourth type of intellectual property protection is a trademark protection. Remember, patents are used to protect inventions and discoveries and copyrights are used to protect expressions of ideas and creations, like art and writing.

Trademarks, then, refer to phrases, words, or symbols that distinguish the source of a product or services of one party from another. For example, the Nike symbol–which nearly all could easily recognize and identify–is a type of trademark.

While patents and copyrights can expire, trademark rights come from the use of the trademark, and therefore can be held indefinitely. Like a copyright, registration of a trademark is not required, but registering can offer additional advantages.

#### Violation: The “inhuman” is not a member nation in the world trade organization, and changing our orientation towards technology is not modifying the law to reduce IP protections -- that was CX.

#### That’s necessary for limits and ground -- redefining portions of the resolution permits endless reclarification AND creates incentives to focus 1 part of the library for 4 years -- only aligning pre-round research with agent and mechanism solves.

#### Two impacts:

#### First is Fairness – prioritize preserving the competitive aspects of debate – games cannot operate unless both sides can be confident in advance they have an equal chance of winning – the fact they’ve asked you to vote for them proves we all agree that debate is a competition.

#### Second is Clash – a common point of engagement ensures effective clash, which is a linear impact – negation is the necessary condition for distinguishing debate from discussion, but negation exists on a sliding scale. The topic of discussion is up to the affirmative, but depth and nuanced engagement is determined by negative ground. Any impact intrinsic to debate, not just discussion, comes from negation because it starts the process of critical thinking, reflexivity, and argument refinement.

#### Clash is key to surviving technological acceleration

Bartanen, Michael D. & R. Littlefield 15, [Michael D. Bartanen, professor of communication at Pacific Lutheran University, and Robert S. Littlefield, NDSU professor of communication.] “Competitive Speech and Debate: How Play Influenced American Educational Practice.” American Journal of Play 7 (2015): 155-173. <https://files.eric.ed.gov/fulltext/EJ1053419.pdf> brett

Competitors broadened their understanding of important social issues and came to understand the role that principled argument played in building a better society. As Progressivism began to emphasize the role of government in checking the power of unfettered capitalism and in ensuring fairness, debate training became a particularly potent tool for contextualizing technical issues. In academic debate, students trained in critical thinking and public speaking more comfortably faced the era’s complex economic and political problems (Bartanen and Littlefield 2014).

#### TVA: Reduce all medical IPs through policy action AND defend changing our orientation towards technology via their method. This is goldilocks because it preserves both their ability to interrogate technology and guarantees negative ground – any 1AR response to the substance of the strategy is offense for us because it proves our model allows for clear contestation and reading the rest of their theory on the negative solves their offense.

## CP

#### Text:

#### States ought to create an international agency monitoring the bioweapons treaty and limit declarations under the biological weapons convention to facilities “especially suitable” for bioweapons uses.

#### States ought to reduce intellectual property protections on medicines to the point that discoverable biological elements are not patentable outside of their country of origin.

#### Solves biowar.

Samore 21. Gary Samore is a Professor of the Practice of Politics and Crown Family Director of the Crown Center for Middle East Studies. This article is republished from The Conversation. BrandeisNOW, “Bioweapons research is banned by an international treaty – but nobody is checking for violations” <https://www.brandeis.edu/now/2021/july/bioweapons-samore.html> sosa

Scientists are making dramatic progress with techniques for “gene splicing” – modifying the genetic makeup of organisms. This work includes bioengineering pathogens for medical research, techniques that also can be used to create deadly biological weapons. It’s an overlap that’s helped fuel speculation that the SARS-CoV-2 coronavirus was bioengineered at China’s Wuhan Institute of Virology and that it subsequently “escaped” through a lab accident to produce the COVID-19 pandemic. The world already has a legal foundation to prevent gene splicing for warfare: the 1972 Biological Weapons Convention. Unfortunately, nations have been unable to agree on how to strengthen the treaty. Some countries have also pursued bioweapons research and stockpiling in violation of it. As a member of President Bill Clinton’s National Security Council from 1996 to 2001, I had a firsthand view of the failure to strengthen the convention. From 2009 to 2013, as President Barack Obama’s White House coordinator for weapons of mass destruction, I led a team that grappled with the challenges of regulating potentially dangerous biological research in the absence of strong international rules and regulations. The history of the Biological Weapons Convention reveals the limits of international attempts to control research and development of biological agents. 1960s-1970s: International negotiations to outlaw biowarfare The United Kingdom first proposed a global biological weapons ban in 1968. Reasoning that bioweapons had no useful military or strategic purpose given the awesome power of nuclear weapons, the U.K. had ended its offensive bioweapons program in 1956. But the risk remained that other countries might consider developing bioweapons as a poor man’s atomic bomb. In the original British proposal, countries would have to identify facilities and activities with potential bioweapons applications. They would also need to accept on-site inspections by an international agency to verify these facilities were being used for peaceful purposes. These negotiations gained steam in 1969 when the Nixon administration ended America’s offensive biological weapons program and supported the British proposal. In 1971, the Soviet Union announced its support – but only with the verification provisions stripped out. Since it was essential to get the USSR on board, the U.S. and U.K. agreed to drop those requirements. In 1972 the treaty was finalized. After gaining the required signatures, it took effect in 1975. Under the convention, 183 nations have agreed not to “develop, produce, stockpile or otherwise acquire or retain” biological materials that could be used as weapons. They also agreed not to stockpile or develop any “means of delivery” for using them. The treaty allows “prophylactic, protective or other peaceful” research and development – including medical research. However, the treaty lacks any mechanism to verify that countries are complying with these obligations. 1990s: Revelations of treaty violations This absence of verification was exposed as the convention’s fundamental flaw two decades later, when it turned out that the Soviets had a great deal to hide. In 1992, Russian President Boris Yeltsin revealed the Soviet Union’s massive biological weapons program. Some of the program’s reported experiments involved making viruses and bacteria more lethal and resistant to treatment. The Soviets also weaponized and mass-produced a number of dangerous naturally occurring viruses, including the anthrax and smallpox viruses, as well as the plague-causing Yersinia pestis bacterium. Yeltsin in 1992 ordered the program’s end and the destruction of all its materials. But doubts remain whether this was fully carried out. Another treaty violation came to light after the U.S. defeat of Iraq in the 1991 Gulf War. United Nations inspectors discovered an Iraqi bioweapons stockpile, including 1,560 gallons (6,000 liters) of anthrax spores and 3,120 gallons (12,000 liters) of botulinum toxin. Both had been loaded into aerial bombs, rockets and missile warheads, although Iraq never used these weapons. In the mid-1990s, during South Africa’s transition to majority rule, evidence emerged of the former apartheid regime’s chemical and biological weapons program. As revealed by the South African Truth and Reconciliation Commission, the program focused on assassination. Techniques included infecting cigarettes and chocolates with anthrax spores, sugar with salmonella and chocolates with botulinum toxin. In response to these revelations, as well as suspicions that North Korea, Iran, Libya and Syria were also violating the treaty, the U.S. began urging other nations to close the verification gap. But despite 24 meetings over seven years, a specially formed group of international negotiators failed to reach agreement on how to do it. The problems were both practical and political. Monitoring biological agents Several factors make verification of the bioweapons treaty difficult. First, the types of facilities that research and produce biological agents, such as vaccines, antibiotics, vitamins, biological pesticides and certain foods, can also produce biological weapons. Some pathogens with legitimate medical and industrial uses can also be used for bioweapons. Further, large quantities of certain biological weapons can be produced quickly, by few personnel and in relatively small facilities. Hence, biological weapons programs are more difficult for international inspectors to detect than nuclear or chemical programs, which typically require large facilities, numerous personnel and years of operation. So an effective bioweapons verification process would require nations to identify a large number of civilian facilities. Inspectors would need to monitor them regularly. The monitoring would need to be intrusive, allowing inspectors to demand “challenge inspections,” meaning access on short notice to both known and suspected facilities. Finally, developing bioweapons defenses – as permitted under the treaty – typically requires working with dangerous pathogens and toxins, and even delivery systems. So distinguishing legitimate biodefense programs from illegal bioweapons activities often comes down to intent – and intent is hard to verify. Because of these inherent difficulties, verification faced stiff opposition. Political opposition to bioweapons verification As the White House official responsible for coordinating the U.S. negotiating position, I often heard concerns and objections from important government agencies. The Pentagon expressed fears that inspections of biodefense installations would compromise national security or lead to false accusations of treaty violations. The Commerce Department opposed intrusive international inspections on behalf of the pharmaceutical and biotechnology industries. Such inspections might compromise trade secrets, officials contended, or interfere with medical research or industrial production. Germany and Japan, which also have large pharmaceutical and biotechnology industries, raised similar objections. China, Pakistan, Russia and others opposed nearly all on-site inspections. Since the rules under which the negotiation group operated required consensus, any single country could block agreement. In January 1998, seeking to break the deadlock, the Clinton administration proposed reduced verification requirements. Nations could limit their declarations to facilities “especially suitable” for bioweapons uses, such as vaccine production facilities. Random or routine inspections of these facilities would instead be “voluntary” visits or limited challenge inspections – but only if approved by the executive council of a to-be-created international agency monitoring the bioweapons treaty. But even this failed to achieve consensus among the international negotiators. Finally, in July 2001, the George W. Bush administration rejected the Clinton proposal – ironically, on the grounds that it was not strong enough to detect cheating. With that, the negotiations collapsed. Since then, nations have made no serious effort to establish a verification system for the Biological Weapons Convention. Even with the amazing advances scientists have made in genetic engineering since the 1970s, there are few signs that countries are interested in taking up the problem again. This is especially true in today’s climate of accusations against China, and China’s refusal to fully cooperate to determine the origins of the COVID-19 pandemic.

#### Solves bioprospecting

Martin Khor October 2000 Why Life Forms Should Not Be Patented Third World Network Features, https://www.twn.my/title/2103.htm

The patenting of living things or life forms, some of which have been made mandatory by the World Trade Organisation, is unethical and also against the economic and social interests of developing countries. Thus, the WTO’s Agreement on trade-related intellectual property rights (TRIPs) should be revised and the patenting of life should instead be prohibited. This was one of the points put forward by speakers and some participants at a panel discussion on the review of the TRIPs Agreement during a seminar on Current Developments in the WTO organised in Geneva by the Third World Network on 14-15 September. The patenting of life forms has become the subject of a growing worldwide campaign by citizen groups, environmentalists, scientists, farmers’ organisations and also religious leaders. They believe that animals, plants, humans, micro-organisms and their parts such as genes and cells, should not be patentable as these life forms are creations of God and Nature. They also argue that life forms, even if they are genetically modified, are not inventions and thus do not meet the criteria of patentability. A debate has also been raging in the WTO, which is reviewing Article 27.3(b) of the TRIPs treaty, which deals with patenting of life forms. It allows countries not to patent plants and animals but makes the patenting of micro-organisms and microbiological processes compulsory, thus opening the road to the patenting of life. Opening the discussion at the TWN seminar, the chairperson, Mr Chakravarthi Raghavan, said that a basic rethinking is now going on in the public arena on the nature of intellectual property rights and TRIPs, on the need to balance the rights of IPR holders and that of users and consumers. Raghavan said policy-makers and negotiators from the South should examine what had been promised in TRIPs on technology transfer and other positive aspects and compare these with the actual results. They should also focus on the aspects of TRIPs that had generated negative effects and that thus need to be reversed. Mr Nelson Ndirangu, a senior Kenyan diplomat based in Geneva, said developing countries had general concerns that TRIPs requires strong regimes to protect intellectual property. The advantage would go to those holding patents. Although the developed countries had said that strong IPR rules would cause technology transfer to take place, five years later this has not happened, and thus the claims of benefit were similar to fraud. In relation to patenting of life forms, Kenya and the Africa Group believes that this is unethical and should not be allowed. This patenting also has serious implications for food security. African countries are not satisfied with Article 27.3(b) of TRIPs. The requirement for protecting micro-organisms, non-biological and microbiological processes and plant varieties is unethical in allowing patents over life forms, unfair in terms of biopiracy, and harms food security for local communities as well as biodiversity. Ndirangu added that when a product is patented, it disallows or discourages research. Big companies that patent would benefit and produce what the market wants. ‘Those of us living on subsistence cannot afford patented products from the North. Also, in relation to products containing genetically modified organisms, we are not sure if they are safe for health or the environment.’ Ms Cecilia Oh, legal adviser to the Third World Network, said that the TRIPs Agreement has contributed to the prevention of access to technology for developing countries. In the case of patents on biological materials, there is a case of ‘double irony’ in that patents are being granted over biological materials and the traditional knowledge of the use of such materials. This prevents access by developing countries to such biological resources and knowledge, which originated largely from the developing countries. In this context, the TRIPs Agreement has facilitated the flow of resources and technology from the South to the North. As the United Nations Conference on Trade and Development (UNCTAD)’s Trade and Development Report 1999 pointed out, IPR protection has generated the outward flow of profits from developing to developed countries, in terms of payments for technology and licensing fees and royalties. Oh said the patent system was not an appropriate reward system for knowledge relating to biological materials. ‘The patent system was designed to protect mechanical inventions, and makes the distinction between mere discoveries and inventions. It is clear that biological materials are naturally occurring and can only be discoveries, and not inventions. ‘Patents confer monopolies over patented subject matter. In the cases of seeds and plant varieties, patents on such biological materials will have serious implications for agriculture and food security in the developing countries. The monopoly over biological resources and knowledge essential for agriculture, medicinal and other uses may be misappropriated and vest in individuals and corporations.’ Oh added that from a scientific perspective, the distinctions made in Article 27.3(b) (for example, between plants and animals, on the one hand, and micro-organisms, on the other) are artificial and were drafted with the aim of allowing and requiring micro-organisms and microbiological processes to be patentable. Quoting from reports made by scientists, Oh said: ‘Scientifically, no such distinctions can be drawn, and therefore, all living organisms and living processes cannot be patentable.’ She said that there are four categories of patents on life forms and processes, which should be prohibited or banned. These are: · Patents based on bio-resources and knowledge of their use pirated from countries and indigenous communities, which do not satisfy the novelty or invention criteria; · Patents on discoveries, for example, micro-organisms, cell lines, genomes, genes (including human cell lines and human genomes and sequences), which are all naturally occurring; · Patents on transgenic techniques and constructs, and transgenic plants, animals and micro-organisms (better known as genetically modified organisms); and · Patents on nuclear transplant cloning (for example, the techniques that produced Dolly the sheep). Oh said: ‘A system for rewards should be developed, but distorting the patent system only serves to attract controversy and rejection of the whole system.’ She added that at the WTO, the African Group of countries has already submitted a comprehensive proposal with the main point ‘that the review process should clarify that plants and animals as well as micro-organisms and all other living organisms and their parts cannot be patented, and that natural processes that produce plants, animals and other living organisms should also not be patentable’. The Africa Group had also proposed that the protection of plant varieties should allow for protection of the innovations of indigenous and local farming communities in developing countries. At discussion time, Mr Leo Palma of the Philippines Mission in Geneva said he subscribed to the view that there should be no patents on life forms. He asked how this principle should be brought forward. A delegate from Trinidad and Tobago said it was important to work out the elements of an appropriate system of protection for plant varieties. A delegate from the India Mission said it was useful to examine the patent application forms and procedures in developed countries, such as the United States. He proposed that in patent application forms a column be added to include the source of origin of biological materials. Before patents are granted, the source of origin as well as evidence whether the knowledge has already been in use should be looked at. This would help prevent patents being granted for products or knowledge that have already been in use in other parts of the world. –

## Case

#### Frame the 1AC through solvency, not impacts – any attempt to filter offense through the RotB or the speech act of the aff is an arbitrary goalpost that only serves to insulate it from criticism and nuanced testing – forcing us to negate the efficacy of personal strategies is at best impossible and at worst violent– no warrant for how the aff spills up to impact structures of politics writ large or out of debate means you vote neg on presumption.

#### Negate on presumption:

#### 1 -- “Affective resistance” is the classic ivory tower academic method that does absolutely nothing – they assume a transformative potential from small moments of resistance that simply does not exist which just plays into the larger structures they criticize

* Also answers their uq question – even if theres an opportunity now, they don’t do anything about it

Reed 16 (Adolph, Jr., Prof. of Political Science @ Penn., “Splendors and Miseries of the Antiracist “Left”” *Nonsite*, http://nonsite.org/editorial/splendors-and-miseries-of-the-antiracist-left-2)

More than a decade and a half ago I criticized similar formulations of a notion of “infrapolitics,” understood as the domain of pre-political acts of everyday “resistance” undertaken by subordinated populations, which was then all the rage in cultural studies programs. Proponents of the political importance of this domain insisted that, because insurgent movements emerge within such cultures of quotidian resistance, a) examining them could help in understanding the processes through which insurgencies develop and/or b) they therefore ought to be considered as expressions of an insurgent politics themselves. Several factors accounted for the popularity of that version of the argument, which mainly had to do to with the political economy of academic life, including the self-propulsion of academic trendiness and the atrophy of the left outside the academy, which encouraged flights into fantasy for the sake of optimism. The infrapolitics idea also resonated with the substantive but generally unadmitted group essentialism underlying claims that esoteric, insider knowledge is necessary to decipher the “hidden transcripts” of the subordinate populations; put more bluntly, elevating infrapolitics to the domain on which the oppressed express their politics most authentically increased its interpreters’ academic capital.8

I discussed those factors in my critique. However, the point in that argument most pertinent for evaluating Birch and Heideman’s confidence that the contradictions they acknowledge in BLM should be seen only as growing pains of a “new movement” is the following:

At best, those who romanticize “everyday resistance” or “cultural politics” read the evolution of political movements teleologically; they presume that those conditions necessarily, or even typically, lead to political action. They don’t. Not any more than the presence of carbon and water necessarily leads to the evolution of Homo sapiens. Think about it: infrapolitics is ubiquitous, developed political movements are rare.9

#### 2 -- There is no exit from information capitalism – their method fails so its try or die to make it work – pespi challenge for a 1ar explanation of how “selective attacks on core nodes” occur and collapse global cap bc there ev sure doesn’t say

-lack of collective action proves

-we depend on global surveillance capitalism, or the ‘world computer’ for daily life---it’s how we get healthcare, communicate with others, get access to services, education, work etc people consider internet access a human right, and networks are organized explicitly to keep them from organizing

Shoshana Zuboff 19, Charles Edward Wilson Professor of Business Administration at the Harvard Business School (retired), where she joined the faculty in 1981, “Surveillance Capitalism and the Challenge of Collective Action,” New Labor Forum, 1/24/19, https://journals.sagepub.com/doi/full/10.1177/1095796018819461

The Challenge to Collective Action

How do they get away with it? Dozens of surveys conducted since 2008 attest to substantial majorities in the United States, the European Union, and around the world that reject the premises and practices of surveillance capitalism, yet it persists, succeeds, grows, and dominates, remaining largely uncontested by either existing or new forms of collective action.28 In other work I have detailed sixteen conditions that enabled this new logic of accumulation to root and flourish.29 Here I want to underscore two of these conditions: The first is the absence of organic reciprocities between surveillance capitalist firms and their populations. This absence produces the second condition, in which dependency replaces reciprocity as the fulcrum of this commercial project.

A first answer to the question “How do they get away with it?” concerns a novel structural feature of this market form that diverges sharply from the history of market democracy. For all the failings, injustice, and violence of earlier forms of modern capitalism, the necessity of organic reciprocities with its populations has been a mark of endurance and adaptability. Symbolized in the twentieth century by Ford’s five-dollar day, these reciprocities reach back to Adam Smith’s original insights into the productive social relations of capitalism, in which firms rely on people as employees and customers. Smith argued that price increases had to be balanced with wage increases “so that the laborer may still be able to purchase that quantity of those necessary articles which the state of the demand for labor … requires that he should have.”30 By the 1980s, globalization and neoliberal ideology, operationalized in the shareholder-value movement, went a long way toward destroying these centuries-old reciprocities between capitalism and its communities. Surveillance capitalism completes the job.

Instrumentarianism is a market project that converges with the digital to achieve its own unique brand of social domination.

First, surveillance capitalists no longer rely on people as consumers. Instead, the axis of supply and demand orients the surveillance capitalist firm to businesses intent on anticipating the behavior of populations, groups, and individuals. The result is that populations are conceptualized as undifferentiated “users,” who are merely the sources of raw material for a digital-age production process aimed at a new business customer. Where individual consumers continue to exist in surveillance capitalist operations—purchasing smart appliances, digital assistants, dolls that spy, or behavior-based insurance policies, just to name a few examples—social relations are no longer founded on mutual exchange. In these and many other instances, products and services are merely hosts for surveillance capitalism’s data extraction operations. For example, the concept of the “smart home” has become emblematic of this new asymmetry. By 2018 the global smart home market was valued at $36 billion USD and expected to reach $151 billion by 2023.31 The numbers betray an earthquake beneath their surface. Consider just one smart home device: the Nest thermostat owned by Alphabet, the Google holding company, and merged with Google in 2018.32 The Nest thermostat collects data about its usage and environment. It uses motion sensors and computation to “learn” the behaviors of a home’s inhabitants. Nest’s apps can also gather data from other connected products such as cars, ovens, fitness trackers, beds.33 Such systems can, for example, trigger lights if an anomalous motion is detected, signaling video and audio recording, and even sending notifications to homeowners or others. As a result of the merger with Google, the thermostat, like other Nest products, will be built with Google’s artificial intelligence capabilities, including its personal digital “Assistant.”34 The thermostat and its brethren devices create immense new stores of knowledge and therefore new power—but for whom?

Wi-Fi-enabled and -networked, the thermostat’s intricate personalized data stores are uploaded to Google’s servers. Each thermostat comes with a “Privacy Policy,” a “Terms of Service Agreement,” and an “End-User Licensing Agreement.” These reveal oppressive privacy and security consequences in which sensitive household and personal information are shared with other smart devices, unnamed personnel, and third parties for the purposes of predictive analyses and sales to other unspecified parties. Nest takes little responsibility for the security of the information it collects and none for how the other companies in its ecosystem will put those data to use.35 A detailed analysis of Nest’s policies by two University of London scholars concluded that were one to enter into the Nest ecosystem of connected devices and apps, each with its own equally burdensome and audacious terms, the purchase of a single home thermostat entails the need to review nearly a thousand so-called contracts.36 Should the customer refuse to agree to Nest’s stipulations, the Terms of Service indicate that the functionality and security of the thermostat will be deeply compromised, no longer supported by the necessary updates meant to ensure its reliability and safety. The consequences can range from frozen pipes to failed smoke alarms to an easily hacked internal home system.37

The absence of consumer reciprocities is complemented by the absence of employment reciprocities. By historical standards the large surveillance capitalists employ relatively few people compared to their unprecedented computational resources. This pattern, in which a small, highly educated workforce leverages the power of a massive capital-intensive knowledge-production infrastructure, is called “hyperscale.”38 The historical discontinuity of the hyperscale business operation becomes apparent by comparing seven decades of General Motors (GM) employment levels and market capitalization to recent post-IPO (initial public offering) data from Google and Facebook. (I have confined the comparison here to Google and Facebook because both were pure surveillance capitalist firms even before their public offerings.)

Nest takes little responsibility for the security of the information it collects and none for how the other companies in its ecosystem will put those data to use.

From the time they went public to 2016, Google and Facebook steadily climbed to the heights of market capitalization, with Google reaching $532 billion by the end of 2016 and Facebook at $332 billion, without Google ever employing more than 75,000 people or Facebook more than 18,000. General Motors took four decades to reach its highest market capitalization of $225.15 billion in 1965, when it employed 735,000 women and men.39 Most startling is that GM employed more people during the height of the Great Depression than either Google or Facebook employs at their heights of market capitalization.

The GM pattern is the iconic story of the United States in the twentieth century, before globalization, neoliberalism, the shareholder-value movement, and plutocracy unraveled the public corporation and the institutions of what historian Karl Polanyi called “the double movement,” a network of “measures and policies … integrated into powerful institutions designed to check the action of the market relative to labor, land, and money.”40 Polanyi’s studies led him to conclude that the operations of a self-regulating market are profoundly destructive when allowed to run free of such countervailing laws and policies. It was the institutions of the double movement that tamed GM’s employment policies with fair labor practices, unionization, and collective bargaining, emblematic of stable reciprocities during the pre-globalization decades of the twentieth century. The societal result was predictable. In the 1950s, for example, 80 percent of adults said that “big business” was a good thing for the country, 66 percent believed that business required little or no change, and 60 percent agreed, “the profits of large companies help make things better for everyone who buys their products or services.”41

[A]…survey in 2015 found 91 percent of respondents disagreeing that the collection of personal information “without my knowing” is a fair tradeoff for a price discount.

Although some critics blamed GM’s institutional reciprocities for its failure to adapt to global competition in the late 1980s, leading eventually to its bankruptcy in 2009, analyses have shown that chronic managerial complacency and doomed financial strategies bore the greatest share of responsibility for the firm’s legendary decline, a conclusion that is fortified by the successes of the German automobile industry in the twenty-first century, where strong labor institutions formally share decision-making authority.42

Nearly seventy years later and in the absence of democratic checks on the power of surveillance capitalists, the picture is very different. For example, a major 2009 survey found that when Americans are informed of the ways that companies gather data for targeted online ads, 73 to 86 percent rejected such advertising.43 Another substantial survey in 2015 found 91 percent of respondents disagreeing that the collection of personal information “without my knowing” is a fair tradeoff for a price discount. Fifty-five percent disagreed that it was a fair exchange for improved services.44 In 2016 PEW Research reported only 9 percent of respondents as very confident in trusting social media sites with their data and 14 percent very confident about trusting companies with personal data. More than 60 percent wanted to do more to protect their privacy and believed there should be more regulation to protect privacy.45

Hyperscale firms have become emblematic of modern digital capitalism, and as capitalist inventions they present significant social and economic challenges, including their impact on employment and wages, industry concentration, and monopoly.46 In 2017 there were 24 hyperscale firms operating 320 data centers with anywhere between thousands and millions of servers (Google and Facebook are among the largest). One hundred more data centers are expected to be online by late 2018. Microsoft invested $20 billion in 2017, and in 2018 Facebook announced plans to invest $20 billion in a new hyperscale data center in Atlanta. According to one industry report, hyperscale firms are also building the world’s networks, especially subsea cables, which means that “a large portion of the global internet traffic is now running through private networks owned or operated by hyperscalers.” In 2016 Facebook and Google teamed up to build a new subsea cable between the United States and Hong Kong, described as the highest-capacity transpacific route to date.47 The surveillance capitalists who operate at hyperscale or outsource to hyperscale operations dramatically diminish any reliance on their societies as sources of employees, and the few for whom they do compete are largely drawn from the most-rarified strata of data science.

The absence of organic reciprocities with people as sources of either consumers or employees is a matter of exceptional importance in light of the historical relationship between market capitalism and democracy. In fact, the origins of democracy in both Britain and America have been traced to these very reciprocities. Even a brief glance at these histories can help us grasp the degree to which surveillance capitalism diverges from capitalism’s past, a divergence in which an extreme structural independence from people lays the foundation for surveillance capitalism’s unique approach to knowledge that we have called “radical indifference.”

In Britain, the rise of volume production and its wage-earning labor force in the nineteenth century contributed not only to workers’ economic power but also to a growing sense of labor’s political power and legitimacy. This produced a new sense of interdependence between ordinary people and elites. Economists Daron Acemoglu and James A. Robinson show that the rise of democracy in nineteenth-century Britain was inextricably bound to industrial capitalism’s dependency on the “the masses” and their contribution to the prosperity made possible by the new organization of production.48

Acemoglu and Robinson conclude that the “dynamic positive feedback” between “inclusive economic institutions” (i.e., institutions defined by reciprocities) and political institutions was critical to Britain’s substantial and non-violent democratic reforms. Inclusive economic institutions, they argue, “level the playing field,” especially when it comes to the fight for power, making it more difficult for elites to “crush the masses” rather than accede to their demands. Reciprocities in economics produced and sustained reciprocities in politics. “Clamping down on popular demands,” they write, “and undertaking a coup against inclusive political institutions would … destroy … [economic] gains, and the elites opposing greater democratization and greater inclusiveness might find themselves among those losing their fortunes from this destruction.”49

The spread of democracy also depended on the reciprocities of consumption, and the American Revolution is the outstanding example of this dynamic. Historian T.H. Breen argues in his path-breaking book, The Marketplace of Revolution, that it was the violation of these reciprocities that set the American Revolution into motion, uniting disparate provincial strangers into a radical new patriotic force. Breen explains that American colonists had come to depend on the “empire of goods” imported from England, and that this dependency instilled the sense of a reciprocal social contract: “For ordinary people, the palpable experience of participating in an expanding Anglo-American consumer market” intensified their sense of a “genuine partnership” with England. Eventually, the British Parliament famously misjudged the rights and obligation of this partnership, imposing a series of taxes that turned imported goods such as cloth and tea into “symbols of imperial oppression.”

Breen describes the unprecedented inventiveness of a political movement originating in the shared experience of consumption, the outrage at the violation of essential producer–consumer interdependencies, and the determination to make “goods speak to power.” The translation of consumer expectations into democratic revolution occurred in three waves, beginning in 1765, when the Stamp Act triggered popular protests, riots, and organized resistance finally expressed in the “nonimportation movement.” (Today we would call it a consumer boycott.)

As Breen tells it, the details of the Act were less important than the colonists’ realization that England did not perceive them as political or economic equals bound in mutually beneficial reciprocities. “By compromising the Americans’ ability to purchase the goods they desired,” he writes, “Parliament had revealed an intention to treat the colonists like second-class subjects,” levying a heavy price “on the pursuit of material happiness.”

In the absence of the organic reciprocities between producers, customers, and employees that bind populations in a shared fate, “user” dependency is the fulcrum of the surveillance capitalist project. Surveillance capitalism spread across the internet just as digital communications became the salient means of social participation. A 2010 BBC poll found that 79 percent of people in twenty-six countries considered internet access to be a fundamental human right.50 Six years later in 2016, the United Nations Human Rights Council would adopt specific language on the importance of internet access.51 In the United States, many people call the emergency services number, 911, on those rare occasions when Facebook is down.52 Most people find it difficult to withdraw from these utilities, and many ponder if it is even possible.53 The result has been an involuntary merger of personal necessity and economic extraction, as the same channels that we rely on for daily logistics, social interaction, work, education, health care, access to products and services, and much more, now double as supply chain operations for surveillance capitalism’s surplus flows. The result is that effective social participation leads through the means of behavioral modification, eroding the choice mechanisms that once adhered to the private realm—exit, voice, and loyalty. There can be no exit from processes that are intentionally designed to bypass individual awareness and on which we must depend for effective daily life. Users lack reliable channels for voice. Loyalty is an empty suit, as participation is better explained in terms of necessity, dependency, helplessness, resignation, the foreclosure of alternatives, and enforced ignorance.

#### 3 -- The NSA bodies leftist hackers.

**DeBoer ’16** [Fredrik; March 15th; Ph.D. from Purdue University; Fredrikdeboer, “c’mon, guys,” http://fredrikdeboer.com/2016/03/15/cmon-guys/]

I could be wrong about the short-term dangers, and the stakes are incredibly high. But in the end we’re left with the same old question: what tactics will actually work to secure a better world?

In a sharp, sober piece about the meaning of left-wing political violence in the 1970s, Tim Barker writes “If you can’t acknowledge radical violence, radicals are reduced to mere victims of repression, rather than political actors who made definite tactical choices under given political circumstances.” The problem, as Barker goes on to imply, is those tactical choices: in today’s America they will essentially never break on the side of armed opposition against the state. The government knows everything about you, I’m sorry to say, your movements and your associations and the books you read and the things you buy and what you’re saying to the people you communicate with. That’s simply on the level of information before we even get to the state’s incredible capacity to inflict violence.

Look, the world has changed. The relative military capacity of regular people compared to establishment governments has changed, especially in fully developed, technology-enabled countries like the United States. The Czar had his armies, yes, but the Czar’s armies depended on manpower above and beyond everything else. The fighting was still mostly different groups of people with rifles shooting at each other. If tomorrow you could rally as many people as the Bolsheviks had at their revolutionary peak, you’re still left in a world of F-15s, drones, and cluster bombs. And that’s to say nothing of the fact that establishment governments in the developed world can rely on the numbing agents of capitalist luxuries and the American dream to damper revolutionary enthusiasm even among the many millions who have been marginalized and impoverished. This just isn’t 1950s Cuba, guys. It’s just not. In a very real way, modern technology effectively lowers the odds of armed political revolution in a country like the United States to zero, and so much the worse for us.

This isn’t fatalism. It doesn’t mean there’s no hope. It means that there is little alternative to organization, to changing minds through committed political action and using the available nonviolent means to create change: a concert of grassroots organizing, labor tactics, and partisan politics. Those things aren’t exactly likely to work, either, but they’re a hell of a lot more plausible than us dweebs taking the Pentagon. Bernie Sanders isn’t really a socialist, but he’s a social democrat that moves the conversation to the left, and if people are dedicated and committed to organizing, the local, state, and national candidates he inspires will move it further to the left still. You got any better suggestions?

Listen, commie nerds. My people. I love you guys. I really do. And I want to build a better world. Not incrementally, either, but with the kind of sweeping and transformative change that is required to fix a world of such deep injustice. But seriously: none of us are ever going to take to the barricades. And it’s a good thing, too, because we’d probably find a way to shoot in the wrong direction. I can’t dribble a basketball without falling down. American socialism is largely made up of bookish dreamers. I love those people but they’re not for fighting. And even if you have a particular talent for combat, you’re looking at fighting the combined forces of Google, Goldman Sachs, and the defense industry. Violence is hard. Soldiering is hard. In an era of the NSA and military robots, it’s really, really hard. “Should we condone revolutionary violence?” is dorm room, pass-the-bong conversation fodder, of precisely the moral and intellectual weight of “should we torture a guy if we know there’s a bomb and we know he knows where it is and we know we can stop it if we do?” It’s built on absurd hypotheticals, propped up by the power of anxious machismo, and undertaken to no practical political end. It’s understandable. I get it, I really do. But it’s got nothing to do with us. The only way forward is the grubby, unsexy work of building coalitions and asking people to climb on board.

#### 4 -- Revealing what computational thinking conceals doesn’t do anything to change the paradigm that drives that relation to technology in the first place.

Torin Monahan 18, UNC communication professor, 4-1-2018, “Algorithmic Fetishism,” https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/10827

Just as proponents of new technological systems are disposed to fetishize them, I worry that scholars and civil society groups run a similarrisk when calling for algorithmic transparency (e.g., ACM 2017; EPIC 2015). From an academic perspective, even a critical one, algorithmic fetishism manifests in the pleasurable pursuit of opening the black box, discovering the code hidden inside, exploring its beauty and flaws, and explicating its intricacies.3It is a technophilic desire for arcane knowledge that can never be grasped completely, so it continually lures one forward into technical realms while deferring the point of intervention. Following from other critiques of transparency projects, it is essential to bear in mind transparency’s roots in scientific epistemic cultures that were from the start limiting and exclusionary (Ananny and Crawford 2016; Haraway 1997; Knorr-Cetina 1999). More than that, calls for transparency resonate strongly with modern scientific rationalities that invite surveillance, quantification, and data analysis as the basis for decision making (Giddens 1990; Porter 1995; Scott 1998). It is a call for surveillance as a corrective to surveillance, which is an iterative mode that never breaks the cycle even when it repeatedly fails to actualize progressive social change (Brucato 2015; Hetherington 2011).While it is critical to open up the black box of algorithmic production, that will always be an insufficient response to the forms of discrimination engendered by them because algorithms cannot be separated from the context of their production and use. They do not act independent of social context, despite alarmist, deterministic narratives about their automated capacities. Racialized algorithmic violence, for instance, cannot be eradicated by tracing down the offending code and splicing it with an uncorrupted variant, as if the domain of computer code was or ever could be a pure dimension free from human prejudices and politics, as if “purity” were not an entirely bankrupt concept in the contemporary conjuncture. Clearly, the violence and prejudice of algorithms is, and always was, an extension of those qualities in societies. So, fetishizing algorithms, even from a critical position, risks sidelining the harder empirical, theoretical, and political work of tracing those links and creating a space for the emergence of more just alternatives.

#### Even if they succeed, state collapse causes loose nukes---extinction.

Milne and Kinsella, 17—Faculty of English, University of Cambridge AND School of Media, Culture and Creative Arts, Faculty of Humanities, Curtin University (Drew and John, “NUCLEAR THEORY DEGREE ZERO, WITH TWO CHEERS FOR DERRIDA,” Angelaki, 22:3, 1-16,) brett

Another version of the “accelerationist” argument captures some of the ideological workings of the term. In Marxist circles, an “accelerationist” is someone who thinks that the collapse of capitalism will be hastened by allowing reactionary forces to speed up capitalism’s self-destruction. There are occasions when such an argument has validity: nothing about the form of the argument makes it inherently or structurally wrong. There are revolutionary moments when allowing capitalism to collapse in order to rebuild a socialist society is a better path than propping up a failing capitalist regime. The judgement is political rather than philosophical. In most contexts, however, the accelerationist argument, especially as a political principle, is deeply dangerous. It would be better, for example, to preserve a failing US capitalist regime while building social forces to take it over, than to allow the nuclear weapons of the United States to fall into the hands of a suicidal military rearguard or some counter-revolutionary terrorist organisation. Preserving the possibility of human life might involve propping up collapsing capitalist institutions, not least the nuclear safety inspectorate, rather than allowing humanity to be swallowed up by some death spiral of presidential dictators in fear of being toppled. These are critical judgements that could arise at any moment, with real risks that poor judgements will hasten a nuclear confrontation that leads to mutually assured annihilation. The formal shape of an accelerationist argument needs to be understood strategically and politically if it is to address nuclear questions.

#### They also link, which demonstrates the aff’s futility---the structure of their argument, the process through which it was written and the context in which they are articulating it in pursuit of the ballot obviously technologize communicative thought---AND their ability to dismiss this by saying sure, but self-awareness and reflexivity inoculates us is precisely why the ballot isn’t key

James Tully 6, “Communication and Imperialism,” CTheory, 2-22-2006, http://ctheory.net/communication-and-imperialism/

Arthur Kroker suggests that the genetic engineering of the “codes” of life in humans and other organic resources, at one end, and the monitoring, surveillance and precision targeting of the global population in space-based network warfare through full spectrum global dominance at the other, represent the two extremes of this way of being in the world (legitimated in terms of “openness” of scientific inquiry and “security” of individuals and the species). Here life itself is pictured as both a network and an object of manipulation and control by informational technologies. Human nature and the environment are absorbed into culture, and so culture/nature is pictured as a kind of standing reserve of manipulable networks. [21] [22] This is not a form of subjectivity and intersubjectivity that a person bears in one particular role among many. It is a communicative habitus that communicators tend to operate within at work and leisure, on the home computer, the cell phone, the wireless laptop, and the BlackBerry. When networkers put these more interactive modes of communication down, they tend to turn to the technology of the communication of “affects”: radio, television, movies and videos. As a result, this worldview and skill set is carried into other areas of life, either colonizing them or disregarding them if they are inaccessible through the network technology. The form of subjectivity and intersubjectivity of network communicators is not an ideology or a worldview in the traditional sense. It is rather the opposite: a mode of being that is skilled in and accustomed to “worldviewing” — surfing through, interacting with and negotiating a kaleidoscope of shifting ideologies and worldviews. Secular modernists, western scientists, indigenous peoples, neo-liberals, non-governmental organizations, anti-globalization activists, hyper-globalisers, deep ecologists, apocalyptic religious fundamentalists in the Bush administration and Bin Laden terrorist networks are all at home in this habitat. Yet, it is not a neutral, all-inclusive medium of communication. It substantially modifies the pre-network forms of subjectivity it includes, transforming them into contingent and malleable worldviews, civilizations, codes, programs, and “scapes”, yet, paradoxically, placing beyond question its own background horizon of disclosure of the world as a complex system of contingent and programmable networks. This taken-for-granted form of subjectification tends to come with the network and goes without saying. It is the characteristic form of subjectivity of network imperialism. We are just beginning to study and make explicit the tacit ways communication networks are re-organizing human subjectivity. Boaventura de Sousa Santos and other critical sociologists of network communication and control argue that the net brings with it, in tandem with programmability, other taken-for-granted ways of organizing and imagining experience, privileging certain forms of communication, communicative rationality, knowledge, problem solving, cooperation and competition, and production and consumption, and discounting or excluding others.[23] Finally, although this is a powerful new form of subjectivity and social ordering, it is one form among many that we bear as modern subjects, and we are not passive recipients of it (as we will see in section 3).

#### Tech innovation undergirded by profit motives are driving the Second Machine Age, which dematerializes capitalism and makes growth a sustainable necessity – they’re right that cybernetics are transforming capitalism, but that’s good

McAfee, 19—cofounder and codirector of the MIT Initiative on the Digital Economy at the MIT Sloan School of Management, former professor at Harvard Business School and fellow at Harvard’s Berkman Center for Internet and Society (Andrew, “Looking Ahead: The World Cleanses Itself This Way,” *More from Less: The Surprising Story of How We Learned to Prosper Using Fewer Resources—and What Happens Next*, Chapter 14, pg 278-292, Kindle, dml)

The decreases in resource use, pollution, and other exploitations of the earth cataloged in the preceding chapters are great news. But are they going to last? It could be that we're just living in a pleasant interlude between the Industrial Era and another rapacious period during which we massively increase our footprint on our planet and eventually cause a giant Malthusian crash.

It could be, but I don't think so. Instead, I think we're going to take better care of our planet from now on. I'm confident that the Second Machine Age will mark the time in our history when we started to progressively and permanently tread more lightly on the earth, taking less from it and generally caring for it better, even as we humans continue to become more numerous and prosperous. The work of Paul Romer, who shared the 2018 Nobel Prize in economics, is one of the sources of this confidence.

Growth Mindset

Romer's largest contribution to economics was to show that it's best not to think of new technologies as something that companies buy and bring in from the outside, but instead as something they create themselves (the title of his most famous paper, published in 1990, is "Endogenous Technological Change"). These technologies are like designs or recipes; as Romer put it, they’re "the instructions that we follow for combining raw materials." This is close to the definitions of technology presented in chapter 7.

Why do companies invent and improve technologies? Simply, to generate profits. They come up with instructions, recipes, and blueprints that will let them grow revenues or shrink costs. As we saw repeatedly in chapter 7, capitalism provides ample incentive for this kind of tech progress.

So far, all this seems like a pretty standard argument for how the first two horsemen work together. Romer's brilliance was to highlight the importance of two key attributes of the technological ideas companies come up with as they pursue profits. The first is that they're nonrival, meaning that they can be used by more than one person or company at a time, and that they don't get used up. This is obviously not the case for most resources made out of atoms—I can't also use the pound of steel that you've just incorporated into the engine of a car—but it is the case for ideas and instructions. The Pythagorean theorem, a design for a steam engine, and a recipe for delicious chocolate chip cookies aren't ever going to get "used up" no matter how much they're used.

The second important aspect of corporate technologies is that they're partially excludable. This means that companies can kind of prevent others from using them. They do this by keeping the technologies secret (such as the exact recipe for Coca-Cola), filing for patents and other intellectual-property protection, and so on. However, none of these measures is perfect (hence the words partially and kind of). Trade secrets leak. Patents expire, and even before they expire, they must describe the invention they're claiming and so let others study it.

Partial excludability is a beautiful thing. It provides strong incentives for companies to create useful, profit-enhancing new technologies that they alone can benefit from for a time, yet it also ensures that the new techs will eventually "spill over"—that with time they’ll diffuse and get adopted by more and more companies, even if that's not what their originators want.

Romer equated tech progress to the production by companies of nonrivalrous, partially excludable ideas and showed that these ideas cause an economy to grow. What's more, he also demonstrated that this idea-fueled growth doesn't have to slow down with time. It's not constrained by the size of the labor force, the amount of natural resources, or other such factors. Instead, economic growth is limited only by the idea-generating capacity of the people within a market. Romer called this capacity "human capital" and said at the end of his 1990 paper, "The most interesting positive implication of the model is that an economy with a larger total stock of human capital will experience faster growth."

This notion, which has come to be called "increasing returns to scale," is as powerful as it is counterintuitive. Most formal models of economic growth, as well as the informal mental ones most of us walk around with, feature decreasing returns—growth slows down as the overall economy gets bigger. This makes intuitive sense; it just feels like it would be easier to experience 5 percent growth in a $1 billion economy than a $1 trillion one. But Romer showed that as long as that economy continued to add to its human capital—the overall ability of its people to come up with new technologies and put them to use—it could actually grow faster even as it grew bigger. This is because the stock of useful, nonrivalrous, nonexcludable ideas would keep growing. As Romer convincingly showed, economies run and grow on ideas.

The Machinery of Prosperity

Romer's ideas should leave us optimistic about the planetary benefits of digital tools—hardware, software, and networks—for three main reasons. First, countless examples show us how good these tools are at fulfilling the central role of technology, which is to provide "instructions that we follow for combining raw materials." Since raw materials cost money, profit-maximizing companies are particularly keen to find ways to use fewer of them. So they use digital tools to come up with beer cans that use less aluminum, car engines that use less steel and less gas, mapping software that removes the need for paper atlases, and so on and so on. None of this is done solely for the good of the earth—it's done for the pursuit of profit that's at the heart of capitalism—yet it benefits the planet by, as we've seen, causing us to take less from it.

Digital tools are technologies for creating technologies, the most prolific and versatile ones we've ever come up with. They're machines for coming up with ideas. Lots of them. The same piece of computer-aided design software can be used to create a thinner aluminum can or a lighter and more fuel-efficient engine. A drone can be used to scan farmland to see if more irrigation is needed, or to substitute for a helicopter when filming a movie. A smartphone can be used to read the news, listen to music, and pay for things, all without consuming a single extra molecule.

In the Second Machine Age, the global stock of digital tools is increasing much more quickly than ever before. It's being used in countless ways by profit-hungry companies to combine raw materials in ways that use fewer of them. In advanced economies such as America's, the cumulative impact of this combination of capitalism and tech progress is clear: absolute dematerialization of the economy and society, and thus a smaller footprint on our planet.

The second way Romer's ideas about technology and growth are showing up at present is via decreased excludability. Pervasive digital tools are making it much easier for good designs and recipes to spread around the world. While this is often not what a company wants—it wants to exclude others from its great cost-saving idea— excludability is not as easy as it used to be.

This isn't because of weaker patent protection, but instead because of stronger digital tools. Once one company shows what's possible, others use hardware, software, and networks to catch up to the leader. Even if they can't copy exactly because of intellectual-property restrictions, they can use digital tools to explore other means to the same end. So, many farmers learn to get higher yields while using less water and fertilizer, even though they combine these raw materials in different ways. Steve Jobs would certainly have preferred for Apple to be the only provider of smartphones after it developed the iPhone, but he couldn't maintain the monopoly no matter how many patents and lawsuits he filed. Other companies found ways to combine processors, memory, sensors, a touch screen, and software into phones that satisfied billions of customers around the world.

The operating system that powers most non-Apple smartphones is Android, which is both free to use and freely modifiable. Google's parent company, Alphabet, developed and released Android without even trying to make it excludable; the explicit goal was to make it as widely imitable as possible. This is an example of the broad trend across digital industries of giving away valuable technologies for free.

The Linux operating system, of which Android is a descendant, is probably the best-known example of free and open-source software, but there are many others. The online software repository GitHub maintains that it's "the largest open source community in the world" and hosts millions of projects. The Arduino community does something similar for electronic hardware, and the Instructables website contains detailed instructions for making equipment ranging from air-particle counters to machine tools, all with no intellectual-property protection. Contributors to efforts such as these have a range of motivations (Alphabet's goals with Android were far from purely altruistic—among other things, the parent of Google wanted to achieve a quantum leap in mobile phone users around the world, who would avail themselves of Google Search and services such as YouTube), but they're all part of the trend of technology without excludability, which is great news for growth.

As we saw in chapter 10, smartphone use and access to the Internet are increasing quickly across the planet. This means that people no longer need to be near a decent library or school to gain knowledge and improve their abilities. Globally, people are taking advantage of the skill-building opportunities of new technologies. This is the third reason that the spread of digital tools should make us optimistic about future growth: these tools are helping human capital grow

#### The consensus of scientists is that innovation will overcome sustainability constraints

Kelly 13 – Cambridge engineering professor (Michael, “Why a collapse of global civilization will be avoided: a comment on Ehrlich & Ehrlich”, July, <http://rspb.royalsocietypublishing.org/content/280/1767/20131193.short#corresp-1>, ldg)

The population explosion (and its Malthusian societal disruptions) that Ehrlich FRS predicted for the 1990s has not come about [5,6], and the concerns in this present Ehrlich paper are not tempered by the mounting evidence of the demographic transition that occurs when the majority of people live in cities and have access to education. In Japan, Europe and North America the population, excluding immigration, is in decline. Some studies indicate that a peak of 9 billion people in 2050 will be followed by a decline to a population of approximately 6 billion in 2100—less than that in 2000 [7] and bringing new problems of unwanted infrastructure assets! The UN is revising its future population estimates downward [8]. If we look at the waste in the contemporary food chain, at the point of growth, in transit to the market and into the homes of consumers, and compound that loss by the amount of food thrown out rather than consumed, we generate the quantity of food to feed the 9 billion today with the systems in place if we were less wasteful and could distribute it [9]. Animal protein is now being generated in the laboratory and not on the farm [10]. Where is the discussion of the impact of mega-cities being self-sufficient in animal protein from factories within their city boundaries 40 years from now? This is the time scale on which synthetic fibre comprehensively displaced wool from most of its markets. Indeed, rather than speak of peak oil, we can speak of peak farmland—we will need smaller areas in future to feed the world, and we will oversee the managed return of excess land to the wild [11]. The starkest example in the consideration of material overconsumption is the smart phone [12]. This was developed within the paradigm of business as usual to improve the way in which we communicate. Two points are relevant. First, the small piece of metal, plastic and semiconductor that fits in the palm of a hand contains the functions of a camera, radio, telephone, answering machine, photo album, dictaphone, music centre, satellite navigation system, video camera and player, compass, stop-watch, Filofax, diary and more, which were all separate and bulky items only 20 years ago. This represents the great dematerialization of modern civilization, well ahead of any imminent collapse of natural resources. The shape of high streets and retail centres are changing to reflect this evolution. Indeed, the recycling of electronic systems will enhance further this capability of doing more with less material, and the market for extended time between recharging has driven extraordinary improvements in energy efficiency. It is these new low-resource technologies with ever-increasing recycled materials that will drive the world in future. Second, the mobile phone is being used in rural Africa and India to inform farmers of optimal times for taking their products to market, thus reducing greatly the loss of product and/or income, and reducing the stress on land from the need to overproduce to compensate for such losses [13]. Peak planet is now the new research topic [14]. Any perceived threat to the security of the energy supply from finite resources over the last 200 years has been met by a deeper search for reserves. Hansen et al. [15], and especially their fig. 6, show just how little (approx. 10%) of the known and accessible fossil fuel reserves (both conventional and unconventional) has been consumed, and we have had 40 years of future energy reserves to hand for some time [16]. We have not stopped looking for more, as with the recent discoveries of huge fields of methyl hydrates. In future, when we leave the fossil fuel age, it will not be because of the exhaustion of fossil fuels, but because a cheaper, cleaner and more convenient alternative technology emerges, and we have ample time, probably 100 years, to get there. Modern climate scientists seem to be fixated on human-produced CO2, and have missed what the Sun [17] and the biosphere [18] have been doing for the last 30 years. If the history of solar behaviour repeats itself and we were to enter another little ice age, every ppm of CO2 in the atmosphere would be a boon as we feed 9 billion people in 2050 compared with the less than 1 billion last time in the seventeenth to eighteenth centuries. The transition out of the Medieval Warm Period into the Little Ice Age harmed but did not collapse global civilization, and we are much better prepared this time. The growing amplitude of the Keeling cycles of CO2 in the atmosphere is evidence of the greening of the biosphere [18]. The present temperature stasis since 1998, if extended by another 5 years, as now suggested [19] at a time of ever-increasing CO2 emissions, implies that both the coupling between CO2 and globally averaged surface temperatures has been exaggerated in the climate models and natural variability has been underestimated. Indeed, Otto et al. [20] have just revised down their estimate of climate sensitivity to atmospheric CO2 to a value that is now half that cited in earlier IPCC reports. Akasofu's [21] projection of the future temperature, made originally in 2000, and based on extending previous climatic cycles without explicit reference to CO2, has been borne out very precisely, and it is more accurate than all the climate model projections put together—furthermore, he makes a projection of lower temperatures until 2030! An over-emphasis on the urgency of mitigation has had a direct societal consequence in the Gadarene rush to reduce fossil fuel consumption. We do have more time to develop proper alternatives to fossil fuels. The current bankruptcies of alternative energy companies are inevitable: their present technology is both immature and uncompetitive. It is an exact repeat of what happened in California in the 1980s in response to the 1970s oil crisis and for the same reasons: without massive subsidy the energy generated did not produce the profits needed to keep up maintenance. (Graphic images of green industrial dereliction can be seen by googling the phrases ‘abandoned solar farms’ and/or ‘abandoned wind farms’.) Two hundred years ago, windmills stopped turning with the advent of steam engines, which were more efficient, needed less maintenance, and provided energy when and where needed. Little has changed in relative terms since! Trends in solar photovoltaics suggest that in 20 years the technology could become absolutely competitive with fossil fuels [22] unless the price of the latter collapses from current high prices just as they did after the 1970s peak. Whatever happens, the total energy from practical and economic solar systems will play a small part in meeting the global energy demand for the foreseeable future: renewable energy sources are intrinsically dilute at source [23]. Energy storage at the large scale is way into the future, except for water for hydroelectricity, as in New Zealand and Norway. Pushing water uphill with alternative energies is woefully inefficient. Communications, new materials and health systems all present humanity with clear opportunities to avoid future problems with tools not available to earlier generations. The Internet, and its implication of all information available everywhere, instantaneously for everyone, will ensure that technical, medical and societal advances will proceed and propagate very rapidly. An advance in one corner of the world will almost instantaneously be accessible and adaptable anywhere. Human travel will change from becoming a necessity to an option, freeing up time, reducing emissions and enhancing business between continents [24]. New ‘designer’ materials and three-dimensional printing technology for manufacture are likely to massively reduce our reliance on depleting natural resources, providing for a far more adaptive approach to materials in applications. The incredible waste we currently produce is likely to reduce very significantly, making for greater resilience against resource depletion [25]. Ehrlich & Ehrlich [1] are concerned about future pandemics in a closely interconnected world. However, advances in medicine and diagnostics will result in significant economic gains in terms of treatment efficacy, in days lost from the workplace and in the ability of mankind to respond to a future pandemic. The recent response to the H5Nn series of bird flu viruses is very encouraging, and the strategies have existed for some time [26]. We can be a much more resilient race in future than we could be in the past. Similarly, with the advances in understanding the brain and President Obama's recent commitment to mapping the brain, we will enhance our cognitive and processing capability so as to further our ingenuity and resilience in response to future threats. The mainstream scientific and engineering community can see nothing that suggests an imminent collapse of civilization, and it is well on track to deal with new problems as they emerge, in continuity with the history of the last 200 years. Neo-Malthusians have proved comprehensively wrong so far, and this comment argues that this is set to continue into the foreseeable future. This comment is not denying challenges, but is really questioning defeatism. Weigh the evidence. Finally, it is only civilizations backed by strong economies that are in a position to do the research and make the necessary scientific, engineering and technological advances to offset environmental threats. Scientific views that undermine economic progress are a threat in themselves, and need a careful and robust justification before they are widely propagated.

#### Cybernetics is key to informatize war---that net reduces violence.

Thomas Rid 13, THOMAS RID is a Reader in War Studies at King’s College London, 12-1-2013, "Cyberwar and Peace," Foreign Affairs, https://www.foreignaffairs.com/articles/2013-10-15/cyberwar-and-peace

Cyberwar Is Coming!” declared the title of a seminal 1993 article by the RAND Corporation analysts John Arquilla and David Ronfeldt, who argued that the nascent Internet would fundamentally transform warfare. The idea seemed fanciful at the time, and it took more than a decade for members of the U.S. national security establishment to catch on. But once they did, a chorus of voices resounded in the mass media, proclaiming the dawn of the era of cyberwar and warning of its terrifying potential. In February 2011, then CIA Director Leon Panetta warned Congress that “the next Pearl Harbor could very well be a cyberattack.” And in late 2012, Mike McConnell, who had served as director of national intelligence under President George W. Bush, warned darkly that the United States could not “wait for the cyber equivalent of the collapse of the World Trade Centers.” Yet the hype about everything “cyber” has obscured three basic truths: cyberwar has never happened in the past, it is not occurring in the present, and it is highly unlikely that it will disturb the future. Indeed, rather than heralding a new era of violent conflict, so far the cyber-era has been defined by the opposite trend: a computer-enabled assault on political violence. Cyberattacks diminish rather than accentuate political violence by making it easier for states, groups, and individuals to engage in two kinds of aggression that do not rise to the level of war: sabotage and espionage. Weaponized computer code and computer-based sabotage operations make it possible to carry out highly targeted attacks on an adversary’s technical systems without directly and physically harming human operators and managers. Computer-assisted attacks make it possible to steal data without placing operatives in dangerous environments, thus reducing the level of personal and political risk. These developments represent important changes in the nature of political violence, but they also highlight limitations inherent in cyberweapons that greatly curtail the utility of cyberattacks. Those limitations seem to make it difficult to use cyberweapons for anything other than one-off, hard-to-repeat sabotage operations of questionable strategic value that might even prove counterproductive. And cyber-espionage often requires improving traditional spycraft techniques and relying even more heavily on human intelligence. Taken together, these factors call into question the very idea that computer-assisted attacks will usher in a profoundly new era. THE THIN CASE FOR CYBERWAR One reason discussions about cyberwar have become disconnected from reality is that many commentators fail to grapple with a basic question: What counts as warfare? Carl von Clausewitz, the nineteenth-century Prussian military theorist, still offers the most concise answer to that question. Clausewitz identified three main criteria that any aggressive or defensive action must meet in order to qualify as an act of war. First, and most simply, all acts of war are violent or potentially violent. Second, an act of war is always instrumental: physical violence or the threat of force is a means to compel the enemy to accept the attacker’s will. Finally, to qualify as an act of war, an attack must have some kind of political goal or intention. For that reason, acts of war must be attributable to one side at some point during a confrontation. No known cyberattack has met all three of those criteria; indeed, very few have met even one. Consider three incidents that today’s Cassandras frequently point to as evidence that warfare has entered a new era. The first of these, a massive pipeline explosion in the Soviet Union in June 1982, would count as the most violent cyberattack to date -- if it actually happened. According to a 2004 book by Thomas Reed, who was serving as a staffer on the U.S. National Security Council at the time of the alleged incident, a covert U.S. operation used rigged software to engineer a massive explosion in the Urengoy-Surgut-Chelyabinsk pipeline, which connected Siberian natural gas fields to Europe. Reed claims that the CIA managed to insert malicious code into the software that controlled the pipeline’s pumps and valves. The rigged valves supposedly resulted in an explosion that, according to Reed, the U.S. Air Force rated at three kilotons, equivalent to the force of a small nuclear device. But aside from Reed’s account, there is hardly any evidence to prove that any such thing happened, and plenty of reasons to doubt that it did. After Reed published his book, Vasily Pchelintsev, who was reportedly the KGB head of the region when the explosion was supposed to have taken place, denied the story. He surmised that Reed might have been referring to a harmless explosion that happened not in June but on a warm April day that year, caused by pipes shifting in the thawing ground of the tundra. Moreover, no Soviet media reports from 1982 confirm that Reed’s explosion took place, although the Soviet media regularly reported on accidents and pipeline explosions at the time. What’s more, given the technologies available to the United States at that time, it would have been very difficult to hide malicious software of the kind Reed describes from its Soviet users. Another incident often related by promoters of the concept of cyberwar occurred in Estonia in 2007. After Estonian authorities decided to move a Soviet-era memorial to Russian soldiers who died in World War II from the center of Tallinn to the city’s outskirts, outraged Russian-speaking Estonians launched violent riots that threatened to paralyze the city. The riots were accompanied by cyber-assaults, which began as crude disruptions but became more sophisticated after a few days, culminating in a “denial of service” attack. Hackers hijacked up to 85,000 computers and used them to overwhelm 58 Estonian websites, including that of the country’s largest bank, which the attacks rendered useless for a few hours. Estonia’s defense minister and the country’s top diplomat pointed their fingers at the Kremlin, but they were unable to muster any evidence. For its part, the Russian government denied any involvement. In the wake of the incident, Estonia’s prime minister, Andrus Ansip, likened the attack to an act of war. “What’s the difference between a blockade of harbors or airports of sovereign states and the blockade of government institutions and newspaper websites?” he asked. It was a rhetorical question, but the answer is important: unlike a naval blockade, the disruption of websites is not violent -- indeed, not even potentially violent. The choice of targets also seemed unconnected to the presumed tactical objective of forcing the government to reverse its decision on the memorial. And unlike a naval blockade, the attacks remained anonymous, without political backing, and thus unattributable. A year later, a third major event entered the cyber-Cassandras’ repertoire. In August 2008, the Georgian army attacked separatists in the province of South Ossetia. Russia backed the separatists and responded militarily. The prior month, in what might have been the first time that an independent cyberattack was launched in coordination with a conventional military operation, unknown attackers had begun a campaign of cyber-sabotage, defacing prominent Georgian websites, including those of the country’s national bank and the Ministry of Foreign Affairs, and launching denial-of-service attacks against the websites of Georgia’s parliament, its largest commercial bank, and Georgian news outlets. The Georgian government blamed the Kremlin, just as the Estonians had done. But Russia again denied sponsoring the attacks, and a NATO investigation later found “no conclusive proof” of who had carried them out. The attack set off increasingly familiar alarm bells within American media and the U.S. national security establishment. “The July attack may have been a dress rehearsal for an all-out cyberwar,” an article in The New York Times declared. Richard Clarke, a former White House cybersecurity czar, warned that the worst was yet to come: the Georgian attack did not “begin to reveal what the Russian military and intelligence agencies could do if they were truly on the attack in cyberspace.” Yet the actual effects of these nonviolent events were quite mild. The main damage they caused was to the Georgian government’s ability to communicate internationally, thus preventing it from getting out its message at a critical moment. But even if the attackers intended this effect, it proved short-lived: within four days after military confrontations had begun in earnest, the Georgian Foreign Ministry had set up an account on Google’s blog-hosting service. This move helped the government keep open a channel to the public and the news media. What the Internet took away, the Internet returned. ISTOCK.COM / -ANTONIO- Overblown: keyboard as grenade. IN CODE WE TRUST? Perhaps the strongest evidence presented by advocates of the concept of cyberwar is the Stuxnet operation launched against Iran by the United States and Israel. Stuxnet, part of a set of attacks known as Operation Olympic Games, was a sophisticated multiyear campaign to sabotage Iran’s nuclear enrichment facility in Natanz by inserting a harmful computer worm into the software that ran the facility’s centrifuges, causing them to overload. American and Israeli developers started designing the project as early as 2005, and it launched in 2007, growing more sophisticated until its discovery in 2010. The attack was groundbreaking in several ways. The developers built highly target-specific intelligence into the code, enabling the Stuxnet software to make autonomous decisions in its target environment. Most important, Stuxnet represented the first and only physically destructive cyberattack launched by one state (or, in this case, two states) against another. Yet even cyberattacks that cause damage do so only indirectly. As an agent of violence, computer code faces a very basic limit: it does not have its own force or energy. Instead, any cyberattack with the goal of material destruction or harming human life must utilize the force or energy embedded in its target: for example, shutting down an air traffic control system and causing trains or planes to crash or disrupting a power plant and sparking an explosion. Yet besides Stuxnet, there is no proof that anyone has ever successfully launched a major attack of this sort. Lethal cyberattacks, while certainly possible, remain the stuff of fiction: none has ever killed or even injured a single human being. Thanks to its lack of direct physical impact, code-induced violence also has less emotional impact. It would be difficult for a cyberattack to produce the level of fear that coordinated campaigns of terrorism or conventional military operations produce. Owing to their invisibility, cyberweapons also lack the symbolic power of traditional ones. Displays of weaponry, such as the elaborate military parades put on by China and North Korea, sometimes represent nothing more than nationalist pageantry. But revealing one’s arsenal can also serve tactical and strategic ends, as when countries deploy aircraft carriers to demonstrate their readiness to use force or carry out operations designed to intimidate the enemy, such as using military aircraft to conduct deliberately low flyovers. Indeed, displaying weapons systems and threatening to use them can prove more cost-efficient than their actual use. But cyberweapons are hard to brandish. Perhaps the most crucial limitation of violence in cyberspace is its almost entirely destructive quality: unlike traditional political violence, which can maintain trust in institutions and states as well as undermine it, violence in cyberspace can do only the latter. Any established political order comes with a certain degree of inherent violence; consolidated states, after all, survive only if they maintain monopolies on the legitimate use of force. By encouraging trust in the ability of state institutions to protect property and safeguard citizens, this inherent violence buttresses a state’s power and allows the state to establish the rule of law. But cyber-violence lacks this ability, since it does little or nothing to build up trust in institutions; indeed, it is very difficult to imagine how cyberattacks could be used to enforce rules or laws, either domestically or internationally. Digital surveillance presents a more complicated picture. In democracies, intelligence agencies tread a thin line between providing security and eroding public trust in the state, as demonstrated by the recent controversy over the U.S. National Security Agency’s data-collection practices. In authoritarian countries, digital surveillance can assist the state’s coercive use of force, but it cannot replace it. Such limitations, however, should not lead anyone to dismiss the corrosive potential of cyberattacks. Indeed, such assaults can undermine social trust in a more direct way than traditional political violence. Cyberattacks are more precise; they do not necessarily undermine the state’s monopoly of force in a wholesale fashion. Instead, they can be tailored to attack specific companies or public-sector organizations and used to undermine those groups’ authority selectively. Stuxnet provides a good example of this dynamic. Putting aside the question of whether the attack was an act of war, its primary intention was to undermine the trust of the Iranian scientists in their systems and in themselves and the trust of the Iranian regime in its ability to build nuclear weapons. The original intention was to cause physical damage to as many Iranian centrifuges as possible. But the American and Israeli attackers knew that the physical effect could be exploited to unleash a much more damaging psychological effect. “The intent was that the failures should make them feel they were stupid, which is what happened,” an American participant told The New York Times. The Americans and the Israelis hoped that once a few machines failed, the Iranian engineers would shut down more machines because they distrusted their own technology or indeed their own skills. At the headquarters of the International Atomic Energy Agency, in Vienna, rumors circulated that the Iranians had lost so much confidence in their own systems and instruments that the management of the Natanz facility took the extraordinary step of assigning engineers to sit in the plant and radio back what they saw to confirm the instrument readings. “They overreacted,” one of the attackers revealed to David Sanger of The New York Times, “and that delayed them even more.” The Iranians also began to assign blame internally, pointing fingers at one another and even firing some personnel. DIGITAL UNDERGROUND Damaging though it may have been, Stuxnet, along with the cyber-scuffles in Estonia and Georgia, represents not a new form of warfare but something more akin to other, less lethal forms of aggression: sabotage and espionage. Unlike acts of war, these political crimes, which are often committed by nonstate actors, need not be violent to work. And although saboteurs and spies do act politically, they often seek to avoid attribution, unlike those who launch acts of war. For those reasons, the cyber-era has been a boon for political crime. Consider sabotage. Before the computer age, saboteurs had trouble calibrating and controlling the effects of their actions. Sabotage had to target physical property and relied on physical violence, which often proves unpredictable. During postal and railway strikes in France in 1909 and 1910, for instance, saboteurs cut signal wires and tore down telegraph posts. Destroying property risked running afoul of public opinion, and the tactic ultimately divided the workers. The strikes themselves, as a form of sabotage, also ran the risk of leading to unpredictable violence: indeed, labor demonstrations often intensified into riots, making it easier for opponents to portray the strikers as uncompromising radicals. It is much easier for saboteurs to avoid counterproductive side effects in the age of computer-assisted attacks, which can contain violence and generally avoid it altogether. Cyberattacks can maliciously affect software and business processes without interfering with physical industrial processes, remaining nonviolent but sometimes still causing greater damage than a traditional assault. A 2012 attack against the computer network of the oil company Saudi Aramco illustrates this potential. The attack physically harmed neither hardware nor humans. Yet by allegedly erasing the hard disks of some 30,000 computers, the attackers likely did much more monetary damage to Saudi Aramco than they could have through an act of traditional sabotage against machinery in one of the company’s plants. The oil giant reportedly had to hire six specialized computer security firms to help with its forensic investigation and post-attack cleanup. Despite such potential, it is also important to remember the inherent limitations of computer-assisted political crime and to note that human agents remain critical in the age of digital violence. Even Stuxnet, the most successful example of cyber-sabotage, demonstrates this fact. For the United States and Israel, the “holy grail,” in the words of one of the attack’s architects, was getting a piece of malicious software into the control system at Natanz. The Americans and Israelis needed fine-grained data from inside the Iranian plant to develop their weaponized code. The problem was that the control system was protected by an air gap: it was not connected to the Internet or even internal networks. As a result, the attackers had to deliver the malicious code via a removable hard drive such as a USB flash drive -- delivered by a human hand. To make this happen, U.S. intelligence operatives first obtained a list of the people who were visiting the targeted plant to work on its computer equipment and who could carry the payload there. “We had to find an unwitting person on the Iranian side of the house who could jump the gap,” one planner later told Sanger. The list of possible carriers included engineers from the German company Siemens, who were helping their Iranian colleagues maintain the control system -- work that required the Siemens engineers to bring portable computers into the plant. Precisely how the U.S.-Israeli team managed to exploit this vulnerability remains unknown. Suffice it to say that although “Siemens had no idea they were a carrier,” in the words of one U.S. official quoted by Sanger, “it turns out there is always an idiot around who doesn’t think much about the thumb drive in their hand.” SAFETY IN ONES AND ZEROS If cyberattacks reduce the amount of violence inherent in conflict, and if they often take the form of sabotage or espionage, then many officials and commentators who have been warning about the dawn of cyberwar have been ringing false alarms. Digital violence does have implications for ethics and for national security strategy, however. Weaponized code, or cyberattacks more generally, can achieve goals that used to require conventional force. The most sophisticated cyberattacks are highly targeted, and cyberweapons are unlikely to cause collateral damage in the same way conventional weapons do. Therefore, in many situations, the use of computers would be ethically preferable to the use of conventional weapons: a cyberattack might be less violent, less traumatizing, and more limited.

#### Cyber tech can be repurposed for ethical means---they foreclose this, propping up dictators

Jan Kallberg 18, research scientist at the Army Cyber Institute at West Point and an assistant professor in the department of social sciences at the United States Military Academy., 8-8-2018, "The case for humanitarian cyber operations," Fifth Domain, https://www.fifthdomain.com/opinion/2018/08/07/the-case-for-humanitarian-cyber-operations/

Cyber operations are designed to be a tool for defense, security and war. In the same way as harmless computer technology can be used as dual-purpose tools for war, tools of war can be used for humanity, to protect the innocent, uphold respect for our fellow beings and safeguard human rights. When a nation-state acts against its population and risks their welfare through repression, violence and exposure to mistreatment, there is a possibility for the world community to take actions by launching humanitarian cyber operations to protect the targeted population. In the non-cyber world, atrocities are intervened by military intervention using the principle of “responsibility to protect,” which allows foreign interference in domestic affairs to protect a population from their repressive and violent ruler without triggering an act of war. If a state fails to protect the welfare of its citizens, then the state that commits atrocities against its population is no longer protected from foreign intervention. Intervention in 2018 does not need to be a military intervention with troops on the grounds, but, instead, a digital intervention through humanitarian cyber operations. A cyber humanitarian intervention not only capitalizes on the digital footprint but also penetrates the violent regime’s information sources, command structure and communications. The growing digital footprint in repressive regimes creates an opportunity for early prevention and interception against the perpetration of atrocities. The last decade the totalitarian states' digital footprint has grown larger and larger. As an example, Iran had 2 million smartphones in 2014, but had already reached 48 million smartphones in 2017. Today, about 3 out of 4 Iranians live in metropolitan areas. About half of the Iranian population is under 30 years old with new habits of chatting, sharing and wireless connectivity. In North Korea, the digital footprint has grown as rapidly. In 2011, there were no cellphones in North Korea outside of a very narrow elite circle. In 2017, surveys assessed that over 65 percent of all North Korean households had a cellphone. No totalitarian and repressive states have been able to limit the digital footprint, which continues to expand for every year. The repressive regimes rely on the computer to lead and orchestrate the repressive actions and crimes against its population. Even if the actual perpetrators of atrocities avoid digital means, the activity will be picked up as intelligence fragments when talked about, discussed, shared, eye-witnessed and silenced. The planning and initiation to execute atrocities have a logistic trail of troop moments, transportations, orders, communications and concentration of resources. If there is a valid concern for the safety of the population in the totalitarian states, then free, democratic and responsible states can act. Utilizing the United Nations' accepted principle, “responsibility to protect,” is a justification for the world community or democratic states that decide to act and to launch humanitarian cyber operations utilizing military cyber capacity in a humanitarian role. Humanitarian cyber operations enable faster response, the retrieval of information is an opportunity embedded in humanitarian cyber operations for humanity and democracy.