Understanding the Information Environment to Win the Next Conflict Without Firing a Shot

Michael Klipstein, Austin Minter, and Jeremiah Pittman

Abstract: In our increasingly digital society, military operations and civilian-alike rely heavily on the technological tools that connect us. Social media has become a powerful influence tool to sow discord, sway sentiment, and purport cause for actions that otherwise would be condemned by the international community. Cellular services have become the default mode of communication. And the amount of data collected continues to grow. The convergence of information operations, electronic warfare, and cyberspace operations have brought a new paradigm to nations in friction or conflict. Distortion and delivery of information allow the perception of 'truth' in populations that in turn can move a nation's course of action. These realities alone are challenging; when US adversaries use cyber capabilities, the result could have a drastic effect on the ability to wage war and retain the status we enjoy in the international community. We examine the holistic information space ten years into the future to better understand how the information environment will interact with governments and society. This paper draws four predictions that will affect nations if the current trend continues. These trends include the diminishment of the United States on the global stage, the rise of China in computing supremacy, cultural division and schism continuing fueled by online news and information sources, and finally, nation-states fighting conflicts further "upstream" in the information space to prevent conflict or eliminate its necessity. In conclusion, the authors recommend questions that governments must seek answers to in order to stay competitive in this environment.

***Index Terms*— cyber warfare, electronic warfare, information operations, online information, persuasion, influence**

I. Introduction

In today's world, smartphones are replacing desktops, laptops, and tablets as the default access point to the Internet. These devices promote increasingly growing access and viewership of non-traditional online news sources who tailor to the bias of the individual viewer; rushing to move and manipulate data online in the 'cloud'; and proliferating connected devices in our lives. As society has digitized, what used to be distinct domains of warfare – cyberwarfare, electronic warfare, and information operations – have converged. Information is delivered via electronic means to digital devices, which are vulnerable to cyberattacks. This reality has changed the way US citizens and soldiers alike receive data, perceive the world, and make decisions.

Powered by the megatrends described above, key indications have emerged: First, adversary narratives will negatively portray the United States to diminish its prestige and influence on the global stage. Second, the Internet of Things (IoT) will continue to proliferate and will be heavily influenced by China's advancement of standards for these platforms; third, that cultural division will increase as news and information sources become tailored for the viewer; and lastly, that countries will seek to move combat "upstream" in the information space in an attempt to avoid kinetic conflict.

II. What Does the Future Hold?

This section examines the predictions made in the introduction: that the US image and influence will be marginalized globally, China will take on a leadership role and have a substantial impact on the development of IoT, curated information sources will increase sectarianism and cultural division, and adversaries will place an increased emphasis on combat in the information space to avoid kinetic conflict. These predictions are built upon the current operational environment but are discussed here in the

This paper was written as part of a DOD Joint Staff Strategic Multilayer Assessment of the future of warfare.

MAJ Michael Klipstein, Ph.D. is a senior researcher and the Chief of Strategic Partnerships at the Army Cyber Institute at West Point, West Point, NY 10996 USA (e-mail: michael.klipstein@westpoint.edu).

CPT Austin Minter is a researcher at the Army Cyber Institute at West Point, West Point, NY 10996 USA (e-mail: Austin.minter@westpoint.edu).

CW3 Jeremiah Pittman is an electronic warfare researcher at the Army Cyber Institute at West Point, West Point, NY 10996 USA (e-mail: jeremiah.pittman@westpoint.edu).

extreme, if the current trajectory continues. Information is vulnerable to cyber operations where it may be denied or manipulated, information operations that serve to manipulate or distort data and context, and electronic warfare where information may be denied, manipulated, or combined with information operations to purposely inject information to a user or group.

A. US prestige and influence on the global stage is marginalized as adversaries illuminate its lack of resolve to maintain superiority.

The United States will continue to leave itself vulnerable in the information space if it lacks a cohesive prescriptive global strategy and operational narrative to guide and communicate the nation's efforts and engagements, particularly with its allies and partners. Reactive strategy lends itself to changing national objectives and, therefore, partner forces losing priority as administrations change. Previous US administrations have ignored the Powell Doctrine, compounding the problem by entering into foreign conflicts without strategy outlining and defining success in the operation.

Adversaries currently weave a tapestry of narratives to diminish US prestige and to attempt to widen schisms with Western allies and partners using multiple tools. Russia (and the Soviet Union) have long used propaganda and other irregular warfare activities as an instrument of national power [1]. For years now, Russia has been setting the stage for conflict with the United States, using its control and influence over the Russian media and other news outlets to propagate the ideas that the United States is the aggressor and that Russia is only protecting its citizens and those of its allies [1, 2, 3]. In the economic space, China's "One-Belt, One Road" initiative has played on the perception that Africa has been exploited by the Western financial system. This narrative has increased China's influence in Africa, helping to displace United States and Western dominance. China's "infrastructure-first" strategy sends economic narratives that showcase how Huawei constructed networks cost as much as 30% less than non-Chinese infrastructures due to China's subsidizing [4]. These economic actions and messages have allowed China to seize an advantage in Africa and developing nations seeking infrastructure support.

Adversaries can and will take advantage of the United States if it turns its back on allies and friends. Even though Georgia had been in talks with the West for admittance to NATO, the international community largely stood by during the Russia-Georgian war in 2008. Scholars have pointed towards US inaction with regarding Georgia as a leading contributor to Russia's invasion of Ukraine and annexation of Crimea six years later, in 2014 [5, 6].

Currently, public discourse over the US withdrawal of forces from Syria in the fight with ISIS is ongoing. Compounding this problem is the presence of Russian military forces in Syria acting on the behest of the Assad government since 1971, while the United States backed rebel forces. Leaving Syria and allowing the Turks to crush the Kurdish partner forces would enable Russia, Iran, and Hezbollah to fill the power vacuum [7] and will send a powerful message to potential strategic partners.

If the United States continues without a cohesive prescriptive global strategy and associated narrative, nations and non-state actors with centralized decision-making authority will continue to use audacity and national will to outpace the decision making of the United States and to portray military restraint as weakness. The restraint shown by US political decision-makers could be portrayed as an unwillingness to project force.

Economically, the US economy will be damaged as its prestige falters and competitors seek to promote themselves on the global stage and build relations with developing and established nations. We see this already with China expanding its influence through the String of Pearls theory along with the IoT and 5G initiatives discussed later in the paper. As US prestige and influence wane on the global stage, competitors filling the power void will seek economic advantages and non-advantageous partnership. Economic impacts will lead to social changes across the international community. Adversary or competitor cultures and influence will rise in locations that once would seek to emulate the United States.

Information and narratives about the United States will be slanted to marginalize and promote an image of weakness and unwilling to commit to defending allies, partner nations, or "free people". Additionally, statements and messaging from the United States will be manipulated to provide "evidence" that the US narrative is false. As other nations promote their presence on the global stage through political actions, economic development, and military action, a committed information campaign will ensue to promote the idea of US weakness and lack of resolve.

B. IoT will continue to proliferate and will be led by China's advancement of standards for these platforms.

China employs a top-down, coordinated effort to lead the world in IoT technology. China has about 500 smart city pilot projects: "Beijing, Shanghai, Guangzhou, Hangzhou, and other large cities have established an extensive database and sensor networks to collect, store, and analyze information related to transportation, electricity, public safety, and environmental factors." [8]. However, China's dominance as a production center has more wide-ranging ramifications as we look at IoT and computing peripherals used in conjunction with cloud storage and manipulation of data.

With smartphones becoming more popular than desktops for Internet access in 2016 and laptops in 2018, mobile phones will continue to be the dominant Internet access platform. Similarly, with smartphones increasing in size and computational power, these devices will continue to become interconnected with other IoT devices and

peripherals in our lives, in the home, car, and work. As smartphones provide a more significant presence in computing because of size, computational power, and convenience, combined with the proclivity for storing and manipulating data in cloud environments [9], China will, therefore, become the de facto leader in data increasing computation. This will be a result of the combination of phones and the growing Chinese population. The sheer impact of China's manufacturing and purchasing power will skew all technological norms in favor of China [10].

Political and military organizations and structures are intertwined in China. Due to the interconnectedness of China's civil-military relations, the intelligence and cyber units of the Chinese People's Liberation Army (PLA) could have access to all of its IoT devices worldwide. The close ties between the government and private companies will also allow China to discover new IoT vulnerabilities that can be leveraged to quickly secure IoT devices against competing intelligence agencies. Many research laboratories are known to directly benefit Chinese military intelligence and cyber operations units. For example, Beijing Key Laboratory of IoT Information Security Technology works directly with the Chinese military. With the proliferation of Chinese made IoT devices, consumers are collecting, sharing, storing, and transmitting troves of data that could be susceptible for use by China's government. China's national security laws currently set a precedent for leveraging Information and Communications Technology for national security uses. The language of these laws though vague in how or when they will be used, explicitly allows Chinese authorities to inspect IT systems and data at will [8].

Economically, China seeks to influence the world to adopt pro-China standards for IoT and 5G technology through both international standards and regional influence initiatives. The US IoT market is expected to reach a market value of $421 billion by 2021 while the Chinese IoT market is expected to reach $264 billion by 2020 with year over year growth expected to continue with rates between 20-30%. The United States and allied nations currently lead overall international market share in IoT technology, but China is quickly gaining and bringing the advantages of its "market size, production capacity, and government support" [8]. Many foreign competitors want to compete in the Chinese market but are blocked or face technology transfer if they enter China due to Chinese business law. China's government-led, predatory market actions, and support for their IoT companies threaten the freedom and opportunities in IoT markets. China is one the most prolific attendees to international technology standards organizations, sending nearly the highest number of delegates to all meetings. Regionally, China is leveraging its Belt and Road Initiative to influence project partner nations to adopt Chinese standards and use Chinese Internet Communication Technology [8]. Since China has the largest potential market for IoT technology, they bring considerable leverage to any standards discussion. This already substantial leverage is magnified when partnered with China's top-down coordination with Chinese companies to undersell foreign competitors in this space [8].

Socially, China will enjoy a monopoly on information and the perception of reality within its borders with a broader control of data and perception of reality abroad. Citizens and visitors alike will be monitored through closed circuit television (CCTV) networks monitoring streets and other public areas. CCTV is already connected to artificial intelligence (AI) and machine learning (ML) allowing for the description of a person through estimated height, weight, age, and clothing worn allowing for correlation against databases to identify the individual in question [11]. These domestic infrastructures will be exported globally and will be discussed with Information.

In terms of infrastructure, by 2025, experts expect 13.8 billion industrial IoT devices with China accounting for 4.1 billion of those. Due to industrial products leading all industries in IoT adoption at 45%, China is perched to dominate the optimization of industrial processes worldwide. China, in particular Huawei, is leading the world in 5G design and production, using AI and data analytics to optimize the industrial sector [12]. China already has "ten times the 5G sites per person as in the United States". This telecommunications backbone sets the stage for IoT devices to be useful. Specifically tailored to IoT devices, Chinese telecom companies have installed over 710,000 specific Narrow Band-IoT base stations. [8]. Compounding China's advantage is the creation of a fiber infrastructure spanning Asia that will only allow Huawei 5G device connections [13]. This infrastructure project will bring economic advantage for nations wishing to connect to the over-land fiber to mitigate fears of the US tapping undersea fiber cables. Additionally, this project's requirement for Huawei devices creates a growing company hegemony that will service almost 70 countries and can service 40% of the world's economic output [13]. With the Belt and Road Initiative bringing high-speed fiber connections to over 800 million homes in China alone, they stand to be the leader in data access and manipulation online.

With its already robust industrial and manufacturing economy, it only makes sense that China would pursue optimization through IoT to cut costs and improve efficiency. The Chinese 5G infrastructure can dynamically create virtual private networks of varying speeds and capacity. When all this data is combined with China's ballooning AI capabilities, China will have the potential to produce the most efficient processes because they will have collected and analyzed the most data. China has already demonstrated predatory market practices in dominating the IoT space; one real danger could be when foreign nations adopt Chinese industrial IoT those systems could be purposefully manipulated to ensure China's economic preeminence.

China's dominance of this space has been synchronized over many years: crafting enduring and long-range strategies within their National Congress, championing adoption of international standards, and through the sheer percentage of global market consumers. These conditions allow China to enjoy a dominant position in the global economy and infrastructure environment. Though China's top-down model of IoT technology promotion incurs significant excess costs, China is committed to leading in the IoT industry because they see this effort as critical both to securing long term economic benefits, and the national security benefits their intelligence community can leverage if they dominate international IoT markets [8].

In the information space, China will continue to control the flow and narrative presented both internally and externally. Using IoT devices, information collection, analysis, and collation will occur at unprecedented levels when coupled with AI and machine learning. China currently employs large scale facial recognition for purposes as diverse as pedestrian law enforcement to purchasing fast food and consumer goods [11]. This always-monitoring capability overlaid with IoT data collection and analysis along with social credit score [14], provides China the ability to track a person in the physical or online world. As China continues to advance IoT standards, the possibility of having a global information collection network becomes a possibility.

C. Cultural division will increase as news and information sources become tailored for the viewer.

The rapid pace of technological change has accelerated the time required to mobilize people, coordinate efforts, and impact an environment. Communication infrastructure, mass media, and society's dependence on technology make it difficult to deny people access to real-time communications, imagery, and video. This technological change has created a virtual world where the real world becomes aware and sentient of everything going on at one instant in time. In this virtual world, geography and transportation no longer limit the space and awareness of things. This enables the warp speed mobilization of humanity and ends with societies becoming divided—mobilizing transnationally to influence whenever stimulated or led.

The core of this technological development revolves around the writing of software and software's ability to enable communication and connectivity in ways that make geography irrelevant. The production of reliable and creative software has thrived in the world allowing for cheap and easy access to technology and the Internet. Unencumbered Internet access will enable groups of people with weak local reference to find others with common values and shared grievances to coalesce around a narrative or perspective that can easily translate to action. The world has realized this during the Arab Spring and the mobilization of transnational terror threats. The advent of increasingly inexpensive devices capable of storage and Internet use in one's pocket has allowed access to become ubiquitous and facilitate greater online dependence resulting in one in five Americans getting their news from social media, more than from print media [15]. Reinforced by confirmation bias, Internet news consumers seek the perspective that more aligns to their personal "truth."

Online news sources have created a phenomenon in which non-traditional news sources have grown in acceptance and viewership due to integration and promotion through social media platforms. In this phenomenon, the race to become the first or most sensational to report has quickened the news cycle for verification, particularly among the non-traditional news providers. An example is the reporting of then President Obama being injured from explosions at the White House [16] resulting in a flash crash of the Dow. With the degradation of journalistic standards, non-traditional news providers are free to publish with impunity.

Politically, online viewership is diluting mainstream media reporting, and combined with confirmation bias, viewers will continue to select news and information outlets that speak to their biases and prejudices causing further societal schisms. As botnets and trolls continue to proliferate narratives supporting or demonizing groups, internal strife will be magnified, and infighting will commence. Outside entities, such as nation-states, will continue to capitalize on this dividing force to weaken national identity and will allow for envelopment of lands, peoples, and natural resources [17]. Social media platforms, and therefore, non-traditional news and information outlets will continue to flourish as governments and organizations use social media to connect with and inform their constituents.

Militarily, narratives will promulgate before operations through social media platforms, and then amplified by non-traditional news and information outlets on social media. This phenomenon is exemplified with ISIS promoting its "overwhelming" victories over the Iraqi government using the hashtag #AllEyesOnISIS [18]. This narrative preceding ISIS forces carried more force than actual ISIS elements, causing Iraqi forces to flee.

Socially, further friction and division will occur between societal groups based on the prejudice du jour. Just as genocide in Rwanda during 1990-1994 was based on conflict between the Hutu and Tutsi, where both groups used irrelevant and often untrue "facts" or "events" to further stoke conspiracy and hatred. Information will become more skewed based on viewership desires and beliefs. Botnets promoting and reinforcing agendas and supporting narratives will continue across social media with even the most isolated locales having access to the Internet and subsequently, "truth." In this information domain, nation-states will work to fight and win conflicts without firing shots—winning through ideas instead of kinetic force.

D. Combatting adversaries will occur farther "upstream" in the information space to avoid kinetic conflict.

Information has long been used to disrupt adversaries, usually individual leaders, through pamphlets or leaflets or transmitted media such as radio or television. The mass populace may have witnessed the message, but the intended recipient was a leader. The ability of one person or group to influence people was proportionate to the resources they could apply. The more resources, the more influence they could have. Currently, one person or one group can influence as many people as they want because technical know-how has all but eliminated proportionate scaling costs.

With the ever-more interconnected world of devices and people, all people will be a target. Leaders will not be the targets of information messaging but instead populations. We see this now with Russian interference in voting for Brexit and the 2016 US presidential election [18]. Projecting forward Gerasimov's ideas for both military and non-military applications of information in conflict [19, 20], this trend will escalate. Countering and proliferating ideas as a precursor to friction or kinetic conflict will increase as the attribution of these actions is difficult. Maintaining deniability as a nation-state while fermenting division in a group will be used to legitimize invasions, reduce internal political risk of a coup, and prevent adversaries from gathering national will for political or military action. As this capability becomes more nuanced and understood, campaign plans spanning in years will emerge to set conditions to attain national objectives. As the Institute for the Future states in their 2018 Report, "Worst of all, since these platforms appear so interactive and democratic, we experience this degradation of our social processes as a form of personal empowerment" [21].

Politically, information warfare can achieve strategic objectives without the expenses and consequences of projection of real military power. Using information warfare and avoiding physical conflict reduces the risk to political careers by avoiding the consequences and attribution of casualties. Political leaders have multiple concepts to diffuse any connection to information warfare campaigns. These operations offer deniability as information warfare tends to use real interest groups and leverages seeds of truth or biases in most campaigns. Leaders can deny involvement in such a campaign, instead blaming information on real interest groups.

The current landscape of weaponized social media platforms to execute information warfare campaigns is extremely complex. Automated social media bots and AI make it increasingly difficult for the public to understand and follow the technical nuances used in larger information warfare campaigns. Targeted messaging to multiple groups has become easier. ISIS has demonstrated how to tailor messages to groups, including using sign language [22]. Technological advancements will continue to make messaging easier, faster, more secure, and non-attributable. Adversaries will choose contentious topics regarding race, gender, national origin, religion, liberal vs. conservative, abortion, sexual preference, ethnicity, or immigration. Any topic that has caused division and foments strong emotional responses for society is a potential candidate for a new information warfare campaign or to falsely promote and magnify a small story.

Militarily, widespread or targeted information warfare campaigns will occur against critical military units or military leaders. An adversary will cause tremendous personal discomfort to many leaders by exposing the contents of his or her personal email, whether real or fabricated. Specific leaders could be "character assassinated" by adversaries planting child pornography on their personal computers, followed by a fraudulent report to authorities or released to the masses. Would there be enough trust in the mainstream media for the public to exonerate a leader falsely accused of these types of charges? Tailored information could be sent directly to troops to erode morale, undermine their cause, or strip away their trust in leadership. This has already been displayed in recent fighting in Ukraine. Tailored and divisive messages were sent directly to frontline Ukrainian troops and their families by Russian-backed separatists. While this was conducted during actual armed conflict, it is not unreasonable to conclude that this would be equally effective prior to open warfare. With the proliferation of technology this new employment of information warfare will be displayed in all phases of future conflict.

Economically, information warfare allows an adversary to achieve a strategic objective with limited investment. With governments utilizing domestic information warfare campaigns, will corporations and private citizens follow suit?

> Nonmilitary forms and means of struggle have received unprecedented development and have acquired a dangerous, sometimes violent nature. The practical use of nonmilitary methods and means can cause a collapse in the energy, banking, economic, information, and other spheres of a state's daily activities. Gerasimov [19]

The United States spends billions in military investments focused on people, air, land, sea, and under-ocean warfare platforms, and infrastructure. But all these military advantages can be superseded by several thousand dollars in computer parts combined with basic technical knowledge and a focused information warfare campaign. This drastically reduces the economic bar to entry into this space. Additionally, with governments utilizing domestic information warfare campaigning, corporations, private citizens, or groups might also follow suit.

Socially, the ubiquity of mobile phones has created a targeted delivery mechanism for nearly every person on earth. If someone does not own a smartphone, his or her network is not worth influencing. Adversaries can easily inject themselves into a social media network and then use sock puppets and botnets to artificially distribute information within that social media group. Original group members, real people assumed to support their group's ideology, following principles of social proof, will begin to accept and spread the new artificial information seeded by adversaries. Inoculating the public to these information campaigns presents unique challenges and the national education environment must foster critical reading and thinking to reduce susceptibility. The Institute for the Future 2018 Report illuminated how disinformation follows contagion propagation models, "Social media manipulates us individually, one private screen at a time...[21].

III. Conclusion

This paper argues that four emerging trends will change the information environment by 2029: the diminishment of America's image and trust on the global stage, the increase of China's influence in IoT and becoming the dominant computing nation, the continued fracturing of societies through cultural schisms brought forth by tailored non-traditional news, and, finally, the shift to combatting adversaries in the information space as a method of avoiding kinetic conflict.

However, the future is not set in stone. To avoid this paradigm and change the future, the United States must draw upon all its resources to ask key questions to understand and successfully navigate this space to create a winning strategy. Such questions include 'What is the number one geopolitical strength and vulnerability of the information environment?' and 'What is the value threshold of real or perceived loss for the administration?' and 'What is the strategic cultural context and priorities of the culture the United States looks to influence?'. This requires the US government to take an introspective look to determine if it can ask better questions of itself, industry, and academia to understand the information environment and the ramifications of actions.

National leaders must create a prescriptive strategy detailing what are the conditions in the information domain the United States will find favorable in the future along with the means and ways to attain them. Additionally, the United States government must engage with industry to prioritize and lead efforts in emerging technologies while investing in domestic production of these technologies. Socially, the United States must have a whole of society effort to adopt and implement these emerging technologies to modernize communications infrastructure with the goal of ranking higher than 7th in the world in the World Bank rankings [23], surpassing Netherlands, Sweden, and Austria. Lastly, the United States must propagate its own messaging of what its goals are and what actions the government will take on the world stage in addition to completing actions when public statements are made to maintain the credibility of the nation and not allow for adversaries to spread a false narrative.

IV. NOTES

[1] S. Jones, "Going on the Offensive: A U.S. Strategy to Combat Russian Information Warfare," Center for Strategic and International Studies, Washington, D.C., 2018.

[2] P. Cobaugh, "A Five-Point Strategy to Oppose Russian Narrative Warfare," Medium Corporation, 04 2018. [Online]. Available: https://medium.com/@paulcobaugh/a-five-point-strateg to-oppose-russian-narrative-warfare-56e0006aab2a. [Accessed 26 02 2019].

[3] The Moscow Times, "Russia's Biggest Enemy Is U.S. – Poll," Moscow Times, 10 01 2018. [Online]. Available: https://www.themoscowtimes.com/2018/01/10/russias-biggest-enemy-is-us-poll-a60146. [Accessed 26 02 201

[4] J. Lewis, "How 5G Will Shape Innovation and Security Center for Strategic and International Studies, Washington, D.C., 2018.

[5] History Channel, "How a Five-Day War With Georgia Allowed Russia to Reassert Its Military Might," History Channel, 08 08 2018. [Online]. Available: https://www.history.com/news/russia-georgia-war-military-nato. [Accessed 25 02 2019].

[6] J. J. Mearsheimer, "Why the Ukraine Crisis is the West' Fault: The Liberal Delusions that Provoked Putin," *Foreign Affairs,* vol. 93, no. 5, pp. 77-89, 2014.

[7] Marwan Kabalan , "What would the US withdrawal fro Syria mean for the region?," Al Jazeera, 23 12 2018. [Online]. Available: https://www.aljazeera.com/indepth/opinion/withdrawal-syria-region-181223131305616.html. [Accessed 23 02 2019].

[8] SOSi, "China's Internet of Things," SOSi, Washington, D,C., 2018.

[9] B. Marr, "9 Technology Mega Trends That Will Chang The World In 2018," 4 12 2017. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2017/12/04/9 technology-mega-trends-that-will-change-the-world-in-2018/#24e81e9e5eed.

[10 New Jersey Insitute of Technology, "Will Mobile Devices Replace Computers," 2019. [Online]. Available https://graduatedegrees.online.njit.edu/resources/mba/m a-infographics/will-mobile-devices-replace-computers/.

[11 Vice, Director, *A Face In The Crowd.* [Film]. 2018.

[12 N. Ismail, "Will China dominate the global industrial Internet of Things market?," 27 06 2018. [Online].

Available: https://www.information-age.com/china-dominate-industrial-iot-123473101/.

[13] Crawford, Susan, "China Will Likely Corner the 5G Market - And the US Has No Plan," 20 02 2019. [Online]. Available: https://www.wired.com/story/china-will-likely-corner-5g-market-us-no-plan/. [Accessed 22 02 2019].

[14] A. Ma, "China has started ranking citizens with a creepy 'social credit' system — here's what you can do wrong, and the embarrassing, demeaning ways they can punish you," 29 10 2018. [Online]. Available: https://www.businessinsider.com/china-social-credit-system-punishments-and-rewards-explained-2018-4.

[15] E. Shearer, "Social media outpaces print newspapers in the U.S. as a news source," 10 12 2018. [Online]. Available: https://pewrsr.ch/2rsoHtb.

[16] P. Domm, "False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitt Feed Was Hacked," 23 04 2013. [Online]. Available: https://www.cnbc.com/id/100646197.

[17] N. A.Mancheri, B. Sprecher, G. Bailey, J. Ge and A. Tukkera, "Effect of Chinese policies on rare earth suppl chain resilience," *Resources, Conservation and Recycling,* pp. 101-112, 28 11 2018.

[18] P. Singer and E. Brookings, Like Wars, New York: Houghton Mifflin Harcourt Publishing, 2018.

[19] V. Gerasimov, "Contemporary Warfare and Current Issues for the Defense of the Country," 1 11 2017. [Online]. Available: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/Contemporary-Warfare-and-Current-Issues-for-the-Defense-of-the-Country.pdf.

[20] V. Gerasimov, "The Value of Science Is in the Foresigh New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," *Military-Industrial Kurier,* 2013.

[21] The Institute for the Future, "The Biology of DIsinformation: Memes, Media Viruses, and Cultural Innoculation," The Institute for the Future, Palo Alto, 2018.

[22] NPR, "Unintended Consequences," 2 11 2018. [Online] Available: https://www.npr.org/programs/ted-radio-hour/662611757/unintended-consequences.

[23] World Bank, "International LPI," World Bank, [Online] Available: https://lpi.worldbank.org/international/global?sort=asc&rder=LPI%20Rank#datatable. [Accessed 23 02 2019].