EMERGING TECHNOLOGIES FOR DISRUPTIVE EFFECTS IN NON-KINETIC ENGAGEMENTS

**Joseph DeFranco,
Diane DiEuliis,
CPT L. R. Bremseth (USN SEAL ret),
LtCol J.J. Snow,
& James Giordano**

Over the past decade, China's increasing activities in media and industrial acquisition, soft power messaging, development, and exploitation of international laws has made it starkly apparent that the U.S. is engaged in an innovative form of multi-dimensional competition. China's commitment to the scientific and technological (S&T) enterprises as specific components of current and future Five-Year Plans emphasize an increasing reliance on—and investment in—convergent S&T approaches (e.g., cyber, nano, media, and economic) to effect dominance on the world stage [1]. This use of multiple technological pathways, coupled with pre-bellicose, non-kinetic actions and subtle yet potent influence operations demonstrates a strategic paradigm to threaten, if not suppress, U.S. global power [2]. During 2018, the Department of Defense (DoD) pressed forward on garnering both internal and external expertise to increase technology-focused efforts necessary to inform policy, acquisitions, and security strategy [3–6]. Over the past four years, the authors were tasked by the Department of Energy's Lawrence Livermore National Laboratory and the Donovan Group and the SOFWERX Innovation Center at United States Special Operations Command (USSOCOM) with studying the use and advantages of current and emerging technologies (ETs) by near-peer adversaries. Toward that end, an exploration of these non-kinetic, technology-enabled engagements was conducted by the group to best define the current evolution in tactics and strategy challenging U.S. national security.

Non-kinetic Engagements

Considerable and expanding aspects of political and military actions directed at adversely impacting (or defeating) an opponent often involve clandestine operations that can be articulated across a spectrum. These operations are frequently augmented by supporting missions that range from overt warfare to far more subtle engagements, which do not meet current criteria for explicit acts of war. Routinely, nations and actors have employed clandestine tactics and operations across kinetic and non-kinetic domains. Arguably, the execution of clandestine kinetic operations is employed more readily, as these collective activities often occur after the initiation of conflict (i.e., "Right of Bang"), and their effects may be observed and/or measured to various degrees. Given that clandestine non-kinetic activities are less visible, they may be particularly effective because they are often unrecognized and occur "Left of Bang." Other nations, especially adversaries, understand the relative economy of force that non-kinetic engagements enable, and are increasingly focused on developing and articulating advanced methods for their operations.

Much has been written about the fog of war [7]. Non-kinetic engagements can create unique uncertainties before and/or outside of traditional warfare, precisely because they have qualitatively and quantitatively "fuzzy boundaries" as blatant acts of aggression [8]. The intentionally-induced ambiguity of non-kinetic engagements can establish plus-sum advantages for the executor(s), and zero-sum dilemmas for the target(s). For example, a limited scale non-kinetic action, which exerts demonstrably significant effects, but does not meet defined criteria for an act of war, places the targeted recipient(s) at a disadvantage. First, in that the criteria for response (and proportionality) are vague and therefore any response could be seen as questionable. Second, in that if the targeted recipient(s) responds with bellicose actions, there is considerable likelihood that

Image Credit | *Photo illustration created by HDIAC and adapted from Adobe Stock.*

they may be viewed as (or provoked to be) the aggressor(s), and therefore susceptible to some form of retaliation that may be regarded as justified.

Non-kinetic engagements often utilize non-military means to expand the effect-space beyond the conventional battlefield. The DoD and Joint Chiefs of Staff do not have a well agreed-upon lexicon to define and to express the full spectrum of current and potential activities that constitute non-kinetic engagements. It is unfamiliar—and can be politically uncomfortable—to use non-military terms and means to describe non-kinetic engagements. And as previously noted, it can be politically difficult, if not precarious, to militarily define and respond to non-kinetic activities.

Disruptive Effects

Non-kinetic engagements are best employed to incur disruptive effects in and across various dimensions (e.g., biological, psychological, social) that can lead to intermediate and long-term destructive manifestations (in a number of possible domains, ranging from the economic to the geo-political). The latent disruptive and destructive effects should be framed and regarded as "Grand Strategy" approaches that evoke outcomes in a "long engagement/long war" context, rather than merely in more short-term tactical situations [9].

> ***"Rapid advances in biotechnology, including gene editing, synthetic biology, and neuroscience, are likely to present new economic, military, ethical, and regulatory challenges worldwide as governments struggle to keep pace..."***
>
> 2019 Worldwide Threat Assessment of the U.S. Intelligence Community to the Senate Select Committee on Intelligence [11]

Thus, non-kinetic operations should be regarded as tools of mass disruption, designed to sustain compounding results that can evoke both direct and indirect de-stabilizing effects. These effects can occur and spread from a) the cellular (e.g., affecting physiological function of a targeted individual) to the socio-political scales (e.g., to manifest effects in response to threats, burdens, and harms incurred by individuals and/or groups), and b) the personal (e.g., affecting a specific individual or particular group of individuals) to the public dimensions in effect and outcome (e.g., by incurring broad scale reactions and responses to key non-kinetic events) [10].

It is important to recognize various nations' dedicated enterprises in developing methods of non-kinetic operations (e.g., China, Russia), and that such endeavors may not comport with ethical systems, principles, and restrictions of the U.S. and its allies [12, 13]. These differing

ethical standards and practices, when coupled to states' highly centralized abilities to coordinate and synchronize activity of the so-called "triple helix" of government, academia, and the commercial sector, can create synergistic force-multiplying effects to mobilize resources and services that can be non-kinetically engaged [14].

Virtual Currencies and Nations

Attention should also be paid to the activities, roles, and viability of virtual currencies and virtual nations as capabilities to exercise disruptive effects and power. The first internet currency, Flooz, was initiated in 1999 [15]. However, it wasn't until 2009 that virtual currencies were actually recognized, and the first blockchain-based cryptocurrency was established [16]. But the true power of virtual currency is in its ability to support smart contracts via the blockchain algorithm.

This strength has allowed legal and medical documents to be uniquely produced and secured while controlling access in a "permissionful" manner. By 2014, virtual nations like BitNation and Asgardia, and countries like Estonia and Bulgaria, began to offer e-residency programs for corporations and digital transients. These new entities offer services and specific benefits to "digital citizens" that may pose unique challenges to traditional governance structures and rules [17–21].

A virtual nation is defined as "an individual, group, community, or corporate entity which derives power from access to high capital resources or high data resources allowing for the influence and successful massing of decentralized digital power to achieve physical effects at the state, national or regional level [22]." A virtual nation may be state- or non-state-sponsored, it may form from collectives, or it may even be a single powerful individual. It is possible that virtual nations may revolutionize how diplomatic, information, military, and economic tools could be used in the future by both state- and non-state actors who are seeking to achieve national- to regional-level effects without being encumbered by traditional laws governing existing nation states [22, 23]. Table 1 provides a comparison of how virtual nations and virtual currencies may enable new mechanisms for the exercise of both power and effect, either in concert or competition with existing nation states, non-state actors, and traditional financial structures.

Blockchain can drive new forms of governance, business, and security by providing a cheap and effective automated mechanism that significantly saves on transaction costs while providing a digital means to formalize relationships between assets, people, and organizations. As well, blockchain can also serve as the foundation for virtual nations. Taken together, virtual currencies and nations can establish bases for multi-dimensional smart contracts [24]. Decentralized Autonomous Organizations are the most complex manifestation of a smart contract. Other features of smart contracts include the ability to self-verify and self-execute; provide improved security; and reduce the need for intermediaries (like existing state governments) to regulate and approve transactions.

This has resulted in the recent revolution of supply chain efficiency by IBM (15% increase in global trade volume, 5% increase in global gross domestic product); secure medical records and real time internal hospital infectious disease detection and tracking by Spiritus Partners; and the successful creation of alternative governance mechanisms that are beginning to rival existing nation state processes and institutions in places like Cyprus, Estonia, and the United Arab Emirates [23]. Such developments can be viewed as economically evolutionary, if not revolutionary, with each and all pushing the boundaries of industry, finance, and governance to significantly change the basis of transactions across domains and dimensions of society [23].

Actor Type	Traditional Financial Structures	Virtual Currency	Governance
Nation State	Primary reliance on traditional financial structures and international markets for daily economic operations	Initial forays include movement toward digital cash in Asia and smart contracts for legal and medical	Five traditional models: monarchy, democracy, oligarchy, authoritarianism, totalitarianism; highly centralized, international law derives from Peace of Westphalia and associated treaties
Non-State/State Sponsored	May relay on traditional financial structures for funding	Movement by certain groups towards alternative financial structures which cannot be frozen or sanctioned by nation states and can be hidden to protect operational security	Centralized or decentralized organizations, ideological or politically focused, may or may not comply with existing governance and/or legal structures; operate within gray zones
Virtual Nations	Will only use traditional financial structures as necessary; tend to avoid reliance on national governance and services in favor of independent and unregulated action	Establish and rely on alternative financial, communication, legal, and decision-making structures frequently based on existing blockchain algorithms, such as Ethereum	Decentralized, borderless, voluntary, self-selecting for code of law, governance type, services provided to citizens and decision-making processes; designed to operate outside of existing Westphalian and international law

Table 1. Characteristics of Real and Virtual Nations and Currencies [23]

Technologies as Enabling Tools in Non-kinetic Engagements

Nation states, virtual nations, and state- and non-state actors' abilities to exert change are enhanced both by: a) radical leveling technologies (RLTs)—extant technologies that can be employed in novel ways to exert disruptive effects in certain contingencies (e.g., changes in social economic markets, vulnerabilities, and volatilities); and b) ETs (i.e., as threats, [ETTs]) that can be utilized for their novel properties and capabilities to exercise multi-focal and multi-scalar disruptions to produce transformative and de-stabilizing effects in support of non-kinetic engagements (see Figure 1). ETs can be particularly problematic given that they are new and may not be viewed or defined as threats, and can evoke effects which, while potent, may not be easily recognizable or attributable to the technology or the actor(s).

Emerging Technologies as Threats

To date, the threat of existing radiological, nuclear, and (high-yield) explosive technologies has been and remains generally well-surveilled and controlled. However, new and convergent

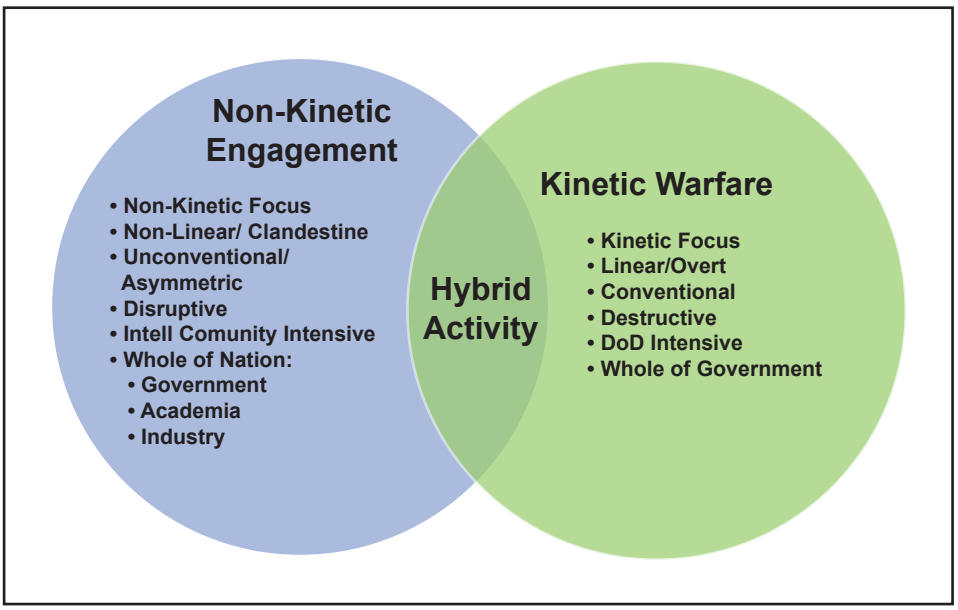

Figure 1. Non-Kinetic and Kinetic Spectrum

Chemical-Biological • Novel drugs and pharmaceutical preparations/delivery systems • Modified microbes (and/or hosts) • Gene-edited benign-to-pathogenic agents (e.g., using CRISPR-Cas9/Cas12) • "Precision" pathologies and immunities • Organic toxins	**Nanotechnologies** • Vectorable, stable nanomaterials
Devices • Directed energy technologies • "Cyborg drones" • Human-machine interfaces	**Biodata** • Manipulable/ targetable information

Table 2. Emerging Technologies as Threats to International/National Security

innovations in the chemical, biological, cybersciences, and engineering fields yield tools and methods that, at present, are not completely or effectively addressed by the Biological Toxin and Weapons Convention (BTWC) or Chemical Weapons Convention (CWC) [25, 1–6]. An overview of these ETs is provided in Table 2.

Our ongoing work focuses primarily upon the brain sciences [10, 13, 25–32]. As recently noted in the *Worldwide Threat Assessment of the US Intelligence Community to the Senate Select Committee on Intelligence* [11], the brain sciences entail and obtain new technologies that can be applied to affect chemical and biological systems in both kinetic (e.g., chemical and biological "warfare" that may sidestep definition—and governance—by the BTWC and/or CWC), or non-kinetic ways (which fall outside of, and, therefore, are not explicitly constrained by the scope and auspices of the BTWC, CWC, or code(s) of conventional warfare) [26–28, 33–34].

Gene Editing

Apropos current events, the use of gene editing technologies and techniques to modify existing microorganisms [35], and/or selectively alter human susceptibility to disease [36], reveals the ongoing and iterative multi-national interest in and weaponizable use(s) of emerging biotechnologies as instruments to produce "precision pathologies" and incur "immaculate destruction" of selected targets. The advent of CRISPR/Cas-based gene editing methods has enabled a more facile approach and has re-enthused interest and capabilities rendered by such techniques. Thousands of guide RNA sequences are broadly available and foster research uses in a variety of health and scientific disciplines [26]. Pairing this new capability to target and study genetic material with other ETs (e.g., neuroscience) could engender the development of potentially hazardous genetic modifications.

Of course, gene editing has limitations. Designing genetically active molecules that can target and affect the DNA in the nucleus of a cell can be arduous. Constructing molecules that are permeable to natural barriers (e.g., the blood-brain barrier, cell membranes, etc.) can be difficult if they are large or chemically inapt. In some cases, these constraints can be overcome both by using ETs or other/older gene editing techniques [37], and as CRISPR/Cas systems continue to increase in utility (i.e., with recent discoveries of additional endonuclease types and subtypes). For example, the Cas12 RNA-guided nuclease effector is a smaller and, in some cases, more functional version of Cas9, which increases the efficacy of CRISPR systems [38].

Indeed, older/alternate gene editing techniques may be used in conjunction with CRISPR/Cas systems to enable more precise genetic targeting. Zinc finger nuclease (ZFN) was one of the first archetypes of enzymatic DNA programing [39]. However, due to difficulties with ZFN design and application, methods like transcription activator-like effector (TALE) and CRISPR/Cas systems were developed for their simplicity and effectiveness [40, 41]. Like CRISPR/Cas systems, TALEs were found to exist in situ within bacteria [42]. The TALE gene editing system has the ability to cleave specific, desirable DNA sequences in various organisms and cell types [43, 44]. Although the technique lacks ease and speed, its high targeting capacity affords various *in vivo* uses. Recent research dedicated to reducing the time required to generate TALE systems may render these applications more facile and viable for use either alone and/or with CRISPR-based approaches in the future [45].

CRISPR/Cas nucleases can be easily programmed to target a DNA segment of interest by pairing them with guide RNA [46]. Currently, CRISPR/Cas-systems are widely recognized as a superior gene editing technology. But like any molecular technique, CRISPR/Cas-based methods can be unsuccessful *in vivo* for numerous reasons. For instance, modifying genetic material can invoke cellular defense mechanisms to repair altered genes (sometimes rendering the modification null) or induce apoptosis (i.e., cell death). Additionally, limited cellular uptake of CRISPR can constrain effects and outcomes. These restrictions have been

overcome in recent studies that have inhibited DNA damage caused by CRISPR/Cas9 [47], or have used gene delivery vectors to enhance uptake and optimize results [48, 49].

Extant unknowns of genomics, proteomics, and neuroscience can both limit CRISPR utility and/or lead to a host of unanticipated (but not necessarily unusable) effects that can be leveraged to influence public health and national security. For example, controlling (if not suppressing) off-target effects is necessary for a successful gene editing system. However, while off-target mutations may be a problem for therapeutics or the enhancement of organisms, such off-target manifestations might not be problematic (or in some cases may be desirable) when using gene editing technology to design a weapon to induce broad-ranging effects.

To be sure, if intended objectives of morbidity or lethality were obtained, it is likely that other (non-morbid or non-lethal) off-target effects would be viewed as less important or disregarded altogether. Further, the use of a combinatory approach (i.e., examining all gene editing systems and/or technologies for their utility) may increase the ease of genetically modifying benign microbes and proteins to be pathogenic, and altering extant pathogens so as to make them more dangerous. These methods could possibly be used to engineer bioagents that evade detection or attribution.

Biodata

CRISPR may also be used to perform rapid, comprehensive screens of specific genes and the phenotypes they produce [50]. This information could be utilized to reveal ways that certain individuals and/or groups could be specifically targeted. We have referred to these various categories of information as "biodata," noting that ETs such as CRISPR, taken with multi-modal information from other forms of assessment (e.g., neuroimaging, biomarkers) have broadened the scope of potential variables that may be identified, accessed, assessed, and, perhaps, ultimately affected [51].

The "digitization of biology" (i.e., information about the genetic code, translated proteins, and/or related metadata) is an unexploited quarry of opportunity for any actor who wishes to specifically target an organism. To be sure, there are concerns about breaches of individual privacy and how such biodata might be interpreted and used to incur certain biases in the ways that individuals or groups are viewed and/or treated. But additional considerations must now be afforded to the risk and threat of physical harms that could be incurred through access to such information.

In this light, biodata may be of even greater concern if and when neuropsychiatrically relevant. Such information could be used to identify individual and group susceptibilities and vulnerabilities to particular agents and effects, which may be instrumental in gene-edited production of novel and more precise microbes, toxins, antigens, or drugs. Moreover, (neuro) biodata can be manipulated to change individual and group medical records in ways that can influence the tenor and scope of clinical care, if not social, legal, and political regard.

Country	Major Research Institutions or Companies	Example Research Projects and Themes
China	• National Center for Nanoscience and Technology • EPRUI Nanoparticles & Microspheres Company • Hongwu International Group	• Biological effects of nanomaterials and nanosafety • Nanodevices, nanomanufacture and applications • Development of nanomaterials and microspheres • Nano-sized powders
Germany	• University of Freiburg • Dresden University of Technology • BASF • Frauenhofer-Gesellschaft	• Bionanotechnology and suprmolecular bioaggregates • Nanoelectronics • Nanoanalyses • Nanostructured materials
Russia	• Moscow Institute of Physics and Technology • RUSNANO • Selecta Biosciences • OCSiAL	• Nanobiopharmaceurtics • Nanooptics and plasmonics • Nanomaterials and quantum nanostructures • Nanoelectronics and photonics
United Kingdom	• University of Cambridge • London Centre for Nanotechnology • ATDBio • Owlstone	• Nanoporous materials • Modifying oligonucleotide scaffolding for nanoengineering • Development of nano-scale structures • Nanofabrication

Table 3. Selected International Nanoengineering Research Programs [55]

Nano-engineering

Nanotechnology is a relatively new science that examines and engineers particles and devices at an atomic or molecular level (1–100 nm). Nanoscience and engineering have been, and are increasingly viewed for their viability to create neurotoxic/neuropathologic agents [34].

A recent review has raised concerns about incomplete effectiveness of protective barriers against the penetrance of nanomaterials to the brain, and this may afford an opportunity for vectoring these substances to the cerebral space to exert a variety of uses [52]. Specifically, attention was focused upon the potential of nanomaterials to induce neuroinflammation, oxidative stress, neuronal cell death, and to alter production of various neuroactive chemicals and affect network properties of the brain.

Evidence shows that nanoparticles can access the central nervous system via a number of routes. Uptake of nanoparticles through the nasal cavity can directly reach the brain through the olfactory tract, and because neurons have the capability to assimilate nanoparticles, the effect can spread throughout the brain. Pulmonary intake involves nanoparticles first crossing the lung-blood barrier, and subsequently the blood-brain barrier, to affect the nervous system. Translocation of nanoparticles from the gut and/or skin to the brain have also been documented, but the efficiency and potency of those routes are less understood [52].

Current applications of nanotechnology include: a) the insertion of nanodevices to remotely control organisms; b) creation of nanocarriers/capsules which could be used to transport molecules (carrying chemicals, proteins, or DNA/RNA) across membranes and the blood-brain barrier to target specific tissues or organs; and c) development of novel neurological molecules that are less (or not) susceptible to current countermeasures and/or therapeutics [53]. Nanomaterials can also be employed to enhance other ETs. As stated above, natural barriers can inhibit or reduce the penetrance and action of CRISPR molecules in the brain, and nanocarriers have been developed to increase the assimilation of

CRISPR molecules into targeted cells [54–56]. Although still under-exploited for its kinetic and non-kinetic potential, nanotechnology is being explored for its dual or direct military use by a number of nations—including the U.S. (see Table 3).

Toward Address, Mitigation, and Prevention

Without philosophical understanding of, and technical insight to, the ways that non-kinetic engagements entail and affect civilian, political, and military domains, coordinated assessment and response to any such engagement(s) becomes procedurally complicated and politically difficult. Therefore, we propose and advocate increasingly dedicated efforts to enable sustained, successful surveillance, assessment, mitigation, and prevention of development and use of RLTs and ETTs to national security.

We posit that implementing these goals will require coordinated focal activities to: a) increase awareness of radical leveraging and ETs that can be utilized as non-kinetic threats; b) quantify the likelihood and extent of threat(s) posed; c) counter identified threats; and d) prevent or delay adversarial development of future threats (see Figure 2).

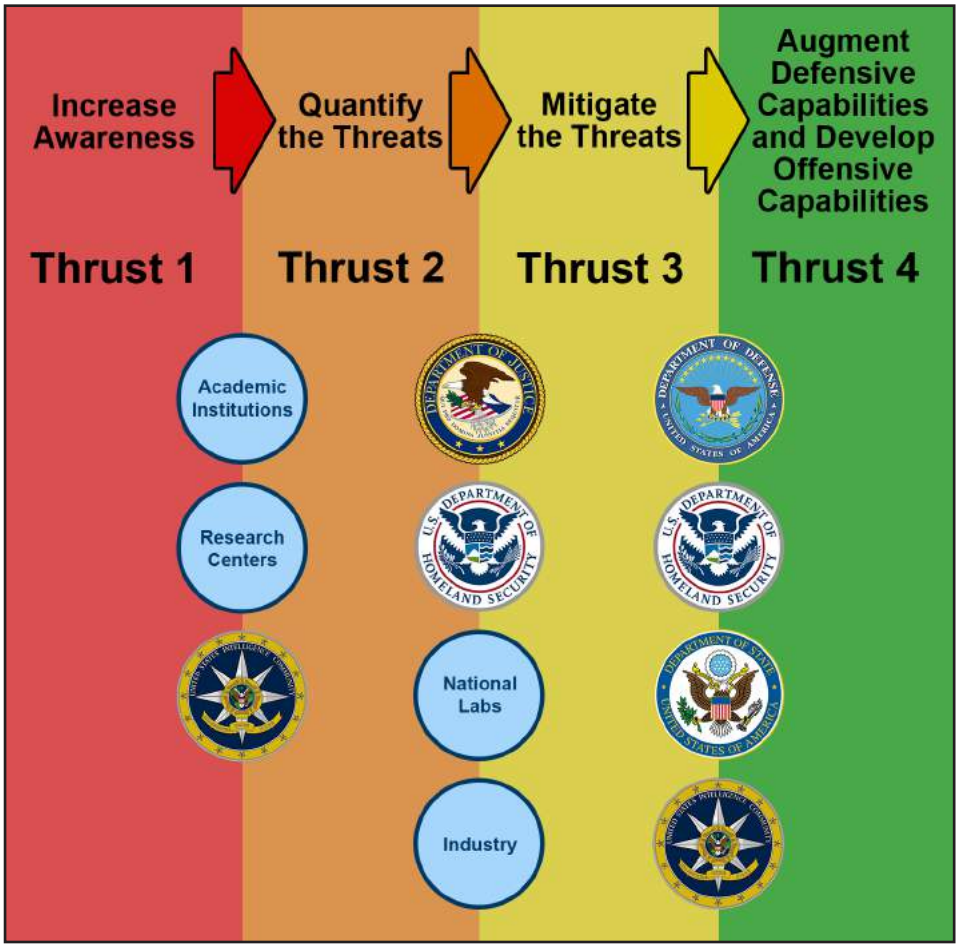

Figure 2. Four-Thrust Whole-of-Nation Approach

Indubitably, there are novel risks associated with misuse of the information and capabilities conferred by RLTs and ETTs. It should be presumed that access to such information and tools by bad actors is high, as many databases are openly shared, and those that are not shared have been, or may be vulnerable to hacking [51]. Access to this information and capability increasingly enables non-kinetic engagements, thereby fortifying the need to identify, meet, assess, and counter novel threats.

Exemplary of such enterprise is the development and growth of a relatively new discipline, "cyber biosecurity," which focuses upon evaluation, mitigation, and prevention of unwanted surveillance, intrusions, and malicious action(s) within cyber systems of the biomedical sciences [57]. However, for cyber biosecurity—or any program of coordinated assessment, mitigation, and prevention—to exert a sustained and iterative effect, it must exist within and be synergized by a larger infrastructure of dedicated effort.

Toward this end, we pronounce the need for a Whole of Nation approach to mobilize the organizations, resources, and personnel required to meet other nations' synergistic triple helix capabilities to develop and non-kinetically engage RLTs and ETTs (see Figure 2).

Utilizing this approach will necessitate establishment of:

1. An office (or network of offices) to coordinate academic and governmental research centers to study and evaluate current and near-future non-kinetic threats

2. Methods to qualitatively and quantitatively identify threats and the potential timeline and extent of their development

3. A variety of means for protecting the U.S. and allied interests from these emerging threats

4. Computational approaches to create and support analytic assessments of threats across a wide range of ETs that may be leveraged and afford purchase in non-kinetic engagements

In light of other nations' activities in this domain, we view non-kinetic deployment of ETs as a clear and viable future threat [11, 58]. Therefore, as previously stated [28, 33, 34], and reiterated here, we believe actions should not focus on whether such methods will be utilized, but rather when, to what extent, and by which group(s) will such use be possible, and most importantly, ensuring the U.S. and its allies will be prepared for these threats when they are rendered.

Disclaimer

The opinions expressed in this article are those of the authors, and do not necessarily reflect those of the United States Department of Defense, United States Special Operations Command, and/or the organizations with which the authors are involved.

Acknowledgements

The authors thank Sherry Loveless for editorial assistance. Support for this work was provided in part by J-5 Donovan Group, USSOCOM (J.D., J.G.); the United States Air Force (J.J.S.); CSCI (L.R.B.; J.G.), and Georgetown University Medical Center (J.G.).

References

1. Choudhury, S. R. (2017, November 12). Chinese M&A: China outbound mergers and acquisitions to rise in 2018. CNBC. Retrieved from https://www.cnbc.com/amp/2017/11/12/chinese-ma-china-outbound-mergers-and-acquisitions-to-rise-in-2018.html
2. Xiu, J., & Daughney, B. C. (2018, October 26). China targeted M&A re-emerges in SPAC world. *New York Law Journal*. Retrieved from https://www.law.com/newyorklawjournal/2018/10/26/china-targeted-ma-re-emerges-in-spac-world/?slreturn=20190307100213
3. U.S. Department of Defense. (2018, December). *Assessment on U.S. Defense Implications of China's Expanding Global Access*. Retrieved from https://media.defense.gov/2019/Jan/14/2002079292/-1/-1/1/EXPANDING-GLOBAL-ACCESS-REPORT-FINAL.PDF
4. Lewis, J. A. (2018, November 30) Technological competition and China. Center for Strategic and International Studies. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/publication/181130_Technological_Competition_and_China.pdf
5. Ferdinando, L. (2018, April 18). DoD must be more agile in technology development, official says. U.S. Department of Defense. DoD News, Defense Media Activity. Retrieved from https://dod.defense.gov/News/Article/Article/1497393
6. Maucione, S. (2019, March 13). DoD 2020 budget puts heavy emphasis on development of emerging technologies. Federal News Radio. Retrieved from https://federalnewsnetwork.com/defense-main/2019/03/dod-2020-budget-puts-heavy-emphasis-on-development-of-emerging-technologies/amp/
7. Owens, W. A., & Offley, E. (2001). *Lifting the Fog of War*. Baltimore, MD: Johns Hopkins University Press.
8. A fuzzy boundary exists within a fuzzy set and describes a concept or condition in which the application can vary according to context or circumstances. See: Haack, S. (1996). *Deviant Logic, Fuzzy Logic: Beyond the Formalism*. Chicago: University of Chicago Press.
9. Davis, Z., & Nacht, M. (Eds.) (2018, February). *Strategic Latency: Red, White and Blue: Managing the National and International Security Consequences of Disruptive Technologies*. Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research. Retrieved from https://cgsr.llnl.gov/content/assets/docs/STATEGIC_LATENCY_Book-WEB.pdf
10. Giordano, J. (2017). Battlescape brain: Engaging neuroscience in defense operations. *Journal of the Homeland Defense & Security Information Analysis Center, 3*(4), 13–16. Retrieved from https://www.hdiac.org/wp-content/uploads/2018/04/CBRN_Battlescape-Brain-Engaging-Neuroscience-in-Defense-Operations-1.pdf
11. Coats, D. (2019). *Worldwide Threat Assessment of the US Intelligence Community to the Senate Select Committee on Intelligence*. Office of the Director of National Intelligence. Retrieved from https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-012919.pdf.
12. Chen, C., Andriola, J., & Giordano, J. (2018, February). Biotechnology, commercial veiling, and implications for strategic latency: The exemplar of neuroscience and neurotechnology research and development in China. In *Strategic Latency: Red, White and Blue: Managing the National and International Security Consequences of Disruptive Technologies*, 12–32. Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research.
13. Palchik, G., Chen, C., & Giordano, J. (2017). Monkey Business? Development, influence, and ethics of potentially dual-use brain science on the world stage. *Neuroethics, 11*(1), 111–114. doi:10.1007/s12152-017-9308-9
14. Etzkowitz, H., & Leydesdorff, L. (2000). The dynamics of innovation: From national systems and "Mode 2" to a triple helix of university-industry-government relations. *Research Policy, 29*(2), 109–123. doi:10.1016/s0048-7333(99)00055-4
15. Higgins, S. (2014, December 1). Three pre-bitcoin virtual currencies that bit the dust. Coindesk. Retrieved from www.coindesk.com/3-pre-bitcoin-virtual-currencies-bit-dust?amp
16. Souli, S. (2016, September 12). I became a citizen of bitnation, a blockchain-powered virtual nation. Now what? Motherboard. Retrieved from https://motherboard.vice.com/amp/en_us/article/xyg5x7/bitnation-or-bust
17. Campbell, R. (2018, March). Screw borders, bitnation lets you create blockchain-powered virtual nations. The Next Web. Retrieved from https://thenextweb.com/cryptocurrency/2018/03/23/screw-borders-bitnation-lets-you-create-blockchain-powered-virtual-nations
18. Gallego, J. (2016, March 11). Bitnation launches the first virtual constitution. Futurism. Retrieved from https://futurism.com/bitnation-launches-worlds-first-virtual-constitution-virtual-nation/amp
19. Lo, A. (2017, November 16). Asgardia, the world's first "space nation," takes flight. CNN. Retrieved from https://www.cnn.com/style/amp/asgardia-satellite-launch/index
20. Harby, B. (2018, August 3). Asgardia: The problems in building a space society. BBC. Retrieved from http://www.bbc.com/future/story/20180803-asgardia-the-problems-in-building-a-space-society
21. Alender, A. (2018, June 20). What is Estonian e-residency and how to take advantage of it? LeapIN. Retrieved from https://www.leapin.eu/articles/e-residency
22. Heimans, J., & Timms, H. (2014, December). Understanding "new power." *Harvard Business Review*. Retrieved from https://hbr.org/2014/12/understanding-new-power
23. Snow, J. (2018, August 27). Dealing with virtual nations: Operating at speed in technology influenced environments. Paper presented at the U.S. Army Training and Doctrine Command (TRADOC) Mad Scientist Initiative meeting, National Intelligence University, Washington, DC.
24. Smart contracts provide a transparent, immutable, iterative mechanism for exchange, verification, and implementation of negotiations and/or functions inherent to a conventional contract. Unlike a conventional contract, they evolve over time to afford flexibility to differentially favor each actor. See: Szabo, N. (1997, September). Formalizing and securing relationships on public networks. *First Monday, 2*(9). Retrieved from https://ojphi.org/ojs/index.php/fm/article/view/548/469
25. Gerstein, D., & Giordano, J. (2017). Rethinking the biological and toxin weapons convention? *Health Security, 15*(6), 638–641. doi:10.1089/hs.2017.0082
26. DiEuliis, D., & Giordano, J. (2017). Why gene editors like CRISPR/Cas may be a game-changer for neuroweapons. *Health Security, 15*(3), 296–302. doi:10.1089/hs.2016.0120
27. Giordano, J. (2017). Weaponizing the brain: Neuroscience advancements spark debate. National Defense, 6, 17-19.
28. Giordano, J., & Wurzman, R. (2011). Neurotechnology as weapons in national intelligence and defense – An overview. *Synesis: A Journal of Science, Technology, Ethics and Policy, 2*, 138–151. Retrieved from http://www.synesisjournal.com/vol2_no2_t1/GiordanoWurzman_2011_2_1.pdf
29. Giordano, J., Forsythe, C., & Olds, J. (2010, April). Neuroscience, neurotechnology, and national security: The need for preparedness and an ethics of responsible action. *AJOB Neuroscience, 1*(2), 35–36. doi:10.1080/21507741003699397
30. Giordano, J. (2016, May 31). The neuroweapons threat. *Bulletin of the Atomic Scientists, 72*(3), 1–4. Retrieved from https://thebulletin.org/2016/05/the-neuroweapons-threat-2/
31. Nixdorff, K., Borisova, T., Komisarenko, S., & Dando, M. (2018, December). Dual-use nano-neurotechnology. *Politics and the Life Sciences, 37*(2), 180–202. doi:10.1017/pls.2018.15
32. Aicardi, C., & Bitsch, L. (2018, December 21). *Opinion on Responsible Dual Use from the Human Brain Project*. Human Brain Project. Retrieved from https://www.humanbrainproject.eu/en/follow-hbp/news/opinion-on-responsible-dual-use-from-the-human-brain-project/
33. Forsythe C., & Giordano, J. (2011). On the need for neurotechnology in the national intelligence and defense agenda: Scope and trajectory. *Synesis: A Journal of Science, Technology, Ethics and Policy, 2*(1), T5–T8. Retrieved from http://www.synesis-journal.com/vol2_no2_t1/Forsythe_Giordano_2011_2_1.pdf
34. Giordano, J. (Ed.) (2015). *Neurotechnology in National Security and Defense: Practical Considerations, Neuroethical Concerns (Advances in Neurotechnology)*. Boca Raton: CRC Press.
35. DiEuliis, D., & Giordano, J. (2017). Gene editing using CRISPR/Cas9: implications for dual-use and biosecurity. *Protein & Cell, 9*(3), 239–240. doi:10.1007/s13238-017-0493-4
36. Belluz, J. (2019, January 22). Is the CRISPR baby controversy the start of a terrifying new chapter in gene editing? Vox. Retrieved from https://www.vox.com/science-and-health/2018/11/30/18119589/crispr-gene-editing-he-jiankui
37. See, for example, Elbashir, S. M., Harborth, J., Lendeckel, W., Yalcin, A., Weber, K., & Tuschl, T. (2001, May 24). Duplexes of 21-nucleotide RNAs mediate RNA interference in cultured mammalian cells. *Nature 411*, 494–498. doi:10.1038/35078107
38. Yan, W., Hunnewell, P., Alfonse, L., Carte, J., Keston-Smith, E., Sothiselvam, S., . . . & Scott, D. (2018). Functionally diverse type V CRISPR-Cas systems. *Science, 363*(6422), 88–91. doi:10.1126/science.aav7271
39. Kim, Y., Cha, J., & Chandrasegaran, S. (1996). Hybrid restriction enzymes: zinc finger fusions to Fok I cleavage domain. *Proceedings of The National Academy Of Sciences, 93*(3), 1156–1160. doi:10.1073/pnas.93.3.1156
40. Nemudryi, A. A., Valetdinova, K. R., Medvedev, S. P., & Zakian, S. M. (2014). TALEN and CRISPR/Cas genome editing systems: Tools of discovery. *Acta Naturae, 6*(3), 19–40. Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4207558/pdf/AN20758251-22-019.pdf
41. Lee, H., Sundberg, B., Sigafoos, A., & Clark, K. (2016, April). Genome ngineering with TALE and CRISPR systems in neuroscience. *Frontiers in Genetics, 7*. doi: 10.3389/fgene.2016.00047
42. Boch, J., Scholze, H., Schornack, S., Landgraf, A., Hahn, S., Kay, S., … & Bonas, U. (2009). Breaking the code of DNA binding specificity of TAL-Type III effectors. *Science, 326*(5959), 1509–1512. doi:10.1126/science.1178811
43. Miller, J. C., Tan, S., Qiao, G., Barlow, K. A., Wang, J., Xia, D. F., . . . & Dulay, G. P. (2011). A TALE nuclease architecture for efficient genome editing. Nature Biotechnology, 29(2), 143–148. doi:10.1038/nbt.1755

44. Joung, J., & Sander, J. (2012). TALENs: A widely applicable technology for targeted genome editing. *Nature Reviews Molecular Cell Biology, 14*(1), 49–55. doi: 10.1038/nrm3486
45. Zhang, S., Chen, H., & Wang, J. (2019, June 14). Generate TALE/TALEN as easily and rapidly as generating CRISPR. *Molecular Therapy: Methods & Clinical Development, 13*, 310–320. doi:10.1016/j.omtm.2019.02.004
46. Dunbar, C., High, K., Joung, J., Kohn, D., Ozawa, K., & Sadelain, M. (2018). Gene therapy comes of age. *Science, 359*(6372), eaan4672. doi:10.1126/science.aan4672
47. Haapaniemi, E., Botla, S., Persson, J., Schmierer, B., & Taipale, J. (2018). CRISPR–Cas9 genome editing induces a p53-mediated DNA damage response. *Nature Medicine, 24*(7), 927–930. doi:10.1038/s41591-018-0049-z
48. Kotterman, M. A., & Schaffer, D. V. (2014). Engineering adeno-associated viruses for clinical gene therapy. *Nature Reviews Genetics, 15*(7), 445. doi:10.1038/nrg3742
49. Gaj, T., Epstein, B. E., & Schaffer, D. V. (2016). Genome engineering using adeno-associated virus: Basic and clinical research applications. *Molecular Therapy, 24*(3), 458–464. doi:10.1038/mt.2015.151
50. Tarasava, K., Oh, E., Eckert, C., & Gill, R. (2018). CRISPR-enabled tools for engineering microbial genomes and phenotypes. *Biotechnology Journal, 13*(9), 1700586. doi:10.1002/biot.201700586
51. DiEuliis, D. (2018). Biodata risks and synthetic biology: A critical juncture. *Journal of Bioterrorism & Biodefense, 09*(01). doi:10.4172/2157-2526.1000159
52. Bencsik, A., Lestaevel, P., & Guseva Canu, I. (2018). Nano- and neurotoxicology: An emerging discipline. *Progress in Neurobiology, 160*, 45–63. doi:10.1016/j.pneurobio.2017.10.003
53. Nasu, H., & McLaughlin, R. (Eds.). (2014). *New Technologies and the Law of Armed Conflict*. The Hague: TMC Asser Press.
54. Lee, B., Lee, K., Panda, S., Gonzales-Rojas, R., Chong, A., Bugay, V., . . . & Lee, H. (2018). Nanoparticle delivery of CRISPR into the brain rescues a mouse model of fragile X syndrome from exaggerated repetitive behaviours. *Nature Biomedical Engineering, 2*(7), 497–507. doi:10.1038/s41551-018-0252-8
55. Lin, Y., Wu, J., Gu, W., Huang, Y., Tong, Z., Huang, L., & Tan, J. (2018). Exosome-liposome hybrid nanoparticles deliver CRISPR/Cas9 system in MSCs. *Advanced Science, 5*(4), 1700611. doi:10.1002/advs.201700611
56. Li, M., Fan, Y., Chen, Z., Luo, Y., Wang, Y., Lian, Z., . . . & Wang, J. (2018). Optimized nanoparticle-mediated delivery of CRISPR-Cas9 system for B cell intervention. *Nano Research, 11*(12), 6270–6282. doi:10.1007/s12274-018-2150-5
57. Peccoud, J., Gallegos, J., Murch, R., Buchholz, W., & Raman, S. (2018). Cyberbiosecurity: From naive trust to risk awareness. *Trends in Biotechnology, 36*(1), 4–7. doi:10.1016/j.tibtech.2017.10.012
58. Pillsbury, M. (2016). *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower*. New York, NY: St. Martin's, Griffin.

Joseph DeFranco
J-5 Donovan Group Fellow, Biowarfare and Biosecurity, United States Special Operations Command (USSOCOM)

Joseph DeFranco is a J-5 Donovan Group Fellow in Biowarfare and Biosecurity, at USSOCOM. He is currently studying neuroscience in the college of arts and sciences, and biodefense at the Schar School of Policy and Government of George Mason University, VA, and formerly served on the staff of Congressman Donald S. Beyer (VA-08). His current research focuses upon the possible use of novel microbiological agents and big data as force-multiplying elements in non-kinetic, hybrid, and kinetic engagements, and the role of global agencies in biosecurity.

Diane DiEuliis, Ph.D.
Senior Research Fellow, National Defense University

Diane DiEuliis, Ph.D., is a Senior Research Fellow of the National Defense University. Her research areas focus on emerging biological technologies, biodefense, and preparedness for biothreats. Specific topic areas within her research portfolio include dual-use life sciences research, synthetic biology, the US bio-economy, disaster recovery, and behavioral, cognitive, and social science as related to important aspects of deterrence and preparedness. Dr. DiEuliis currently has several research grants in progress, and guest lectures in a variety of foundational professional military education courses.

CPT L.R. Bremseth, (USN SEAL ret)
Senior Special Operations Advisor, CSCI

CPT L.R. Bremseth (USN SEAL [ret]) serves as the Senior Special Operations Advisor for CSCI, a strategic support organization in Springfield, VA. He previously served as the Deputy Senior Director of the Integration Support Directorate (ISD) for the Department of the Navy (DON). As such, he was a key advisor to the Secretary, Under Secretary and Deputy Under Secretary of the Navy for sensitive activities. CPT Bremseth was appointed to the Defense Intelligence Senior Level, and Director, Operations and Executive Director prior to his appointment as Deputy Senior Director, ISD. He retired from the Navy in 2006 with 29 years of service, during which he commanded SEAL Team EIGHT (1996–1998) and served a major command tour at Naval Special Warfare Group THREE (2003–2005).

LtCol J.J. Snow
Donovan Group Innovation Officer, United States Special Operations Command (USSOCOM)

LtCol Jennifer "JJ" Snow, USAF, is the Donovan Group Innovation Officer for the USSOCOM, J52 Futures Plans and Strategy Division and SOFWERX Team. She serves as the military representative for technology outreach and engagement to bridge the gap between government and various technology communities to improve collaboration and communications, identify smart solutions to wicked problems and help guide the development of future smart technology policy to benefit special operations.

James Giordano, Ph.D.
Chief of the Neuroethics Studies Program, Pellegrino Center for Clinical Bioethics

Senior author, James Giordano, Ph.D., is a professor in the Departments of Neurology and Biochemistry, Chief of the Neuroethics Studies Program of the Pellegrino Center for Clinical Bioethics, and Co-Director of the O'Neill-Pellegrino Program in Brain Sciences and Global Law and Policy. As well he is J-5 Donovan Group Senior Fellow, Biowarfare and Biosecurity, at United States Special Operations Command. He has served as Senior Science Advisory Fellow to the SMA Group of the Joint Staff of the Pentagon; as Research Fellow and Task Leader of the EU-Human Brain Project Sub-Program on Dual-Use Brain Science, and as an appointed member of the Neuroethics, Legal and Social Issues Advisory Panel of the Defense Advanced Research Projects Agency. He is an elected member of the European Academy of Science and Arts, and a Fellow of the Royal Society of Medicine (UK).