White Paper: A New U.S. National Security Act for the 21st Century

by

Dr. Charles M. Russo, IFPC

Ms. Stella Micholitsi, MA

Mr. Michael Drake Jones, MA

**National security is** a sentiment quantified by the unified actions of a nation and, to some extent, the expectation of its allies. National security spans the limits of a nation’s sovereign territory, the cyberspace domain, and the global economy, just to name a couple. While the citizenry's actions influence national security, it is ultimately executed by intense work of the executive, legislative, and judicial branches of the government, including policymaking, intelligence, and the armed forces, under the supervision of such agencies defined by the Constitution of the United States. Those actions include protection from espionage in all aspects of vital national security intellectual and physical property. Moreover, national security is characterized by all those collective actions starting from low-level decision-making to the strategic level that anticipate and ultimately achieve to protect from harmful practices that additionally and progressively contribute to vulnerability. National security is the unifying declaration of all Americans committed to safeguarding the identity and interests of the Nation, regardless of political orientation and agendas. National security exceeds individual interests and prioritizes the collective wellbeing of the United States, offering its allies a robust global power that they can rely on as a stabilizing factor.

**Four Pillars of National Security Act (NSAct): Mindfulness – Proactiveness- Expertise – Flexibility**

The existence and safeguarding of the U.S. depend on the intention, thoughts, and implementation of its strategic policy. The basis of democracy, unity of effort (E Pluribus Unum), and freedom are the core principles defining the NSAct. It will encompass domestic and foreign elements, ranging from the decisions in one’s public life to a nation’s strategic policies, bilateral/multilateral relations, and behavior in international organizations. The NSAct is the backbone and fundamental pillar of the function of the state, the agencies manifesting its policy, and it must have the population’s understanding and support.  The NSAct will have to face domestic and internationally connected challenges that act as communicating vessels, igniting, or putting out the fire of instability and insecurity. The NSAct should serve well-structured guidelines with no margins left for misinterpretation or legal manipulation while also providing well-bonded legal document flexibility. It must have such clarity and unity that it will be impossible to be affected by political agendas that may shift during election cycles. At the same time, it must be prone to following strategic policy agendas to face challenges when they occur.

**The NSAct in the world of dramatically changing threats and challenges**

The following 75 years may surprise the world with massive disruptions in how life is considered normal due to environmental challenges and displayed aggressiveness by powerful states (cyber or kinetic). The overall concept should be to survive with or without advanced technology. In the first situation where technology thrives, cyber wars and offensives will be part of any declared or undeclared war; therefore, the Office of the Director of National Intelligence (ODNI) should have direct access to updates by a Director of Cyber Intelligence (DCI) overseeing and coordinating all cyber responsibilities such as Department of Defense (DoD), the Central Intelligence Agency and the Federal Bureau of Investigation. This would not mean tampering with the way they function, causing more bureaucracy, but rather the one person with deep knowledge that can warn, take action against trends, and steer the early warning system of cyber defense. At the same time, the DCI could create a continuity plan for functioning after a far-reaching network collapse and the return to a pre cyberspace era. This would prevent people from panicking and the economy from collapsing. As a chain reaction to the above, the NSAct should prepare for natural disasters and the inability to communicate by developing a “**National Sustainability Structure**” that would require the collaboration of the following sectors or departments: Education, Agricultural, Energy/Climate Change, Research & Development (R&D), Commerce/Logistics, and the U.S. Department of Human Health and Services. Those departments should constantly collaborate for the following reasons. The U.S. Department of Education should form a curriculum for young children to address citizen responsibilities, cyber education that focuses on self-protection and exposure, communication without a network, the impact of individual daily habits on climate change, and critical thinking over emergencies subsequent procedures. The agricultural sector should monitor the nation’s storage and supply chain for food and water that would have to be autonomous from imports. Energy and Climate change, along with R&D, will have to produce and implement environment-friendly practices that, in case of an emergency apart from oil and gas, use geothermal energy, which will have to be accessible and cheaper. Commerce and Logistics will have to ensure the continuity of supplies across the U.S. and assist allies as U.S. aid. Finally, the health department must expect and prepare for more global diseases and pandemics for two reasons. First, it is a natural phenomenon that controls the population, and second, it is because of human arrogance, undeclared biological wars, and experiments. Healthy diet campaigns as a proactive measure from a very early age are the key to developing populations with strong immune systems. This must be implemented along with the Department of Education. Ultimately, the U.S. must activate what law professor Jay P. Kesan describes as “active self-defense,” even by referring to cyber matters. (Kesan, 2011)

In 1945, Secretary of War Henry Stimson said, “…the disciplined, trained, and patriotic citizenry of a nation remain the bricks of the foundation upon which the other methods and means of security rest…..there are now *attaches* to the United States as a great world power…to meet our obligation of bearing our full share in preserving world peace…” (Cohen, 2019, p. 157).

**Effects of globalization, changes in world dynamics, and waning days of individual democracies**

Globalization has made its manifestation through the economy, communication, cyberspace, and pandemics that spread quickly through the connectivity of the vast majority of people. Moreover, it has made the migration phenomenon more intense and achievable in people discontent with their countries of origin. The interconnection reinforces the latter through cyberspace. Current shortcomings like right and left-wing extremism manifest themselves and trigger internal discontent, exacerbating extreme behaviors. Moreover, while technology has boosted the intelligence collection capabilities, the enormous amount of data is almost impossible to process and cross-examine by agencies that could monitor and identify nefarious networks. The United States Intelligence Community (USIC) structure has become tortuous and multilayered in approval and oversight. There is no need for overwhelming oversight. There needs to be a choice between the Congressional Defense Committees, the Permanent Select Committee on Intelligence (House of Representatives and the Select Committee on Intelligence of the Senate), or an entirely new smaller Committee that combines much fewer people from the previous ones.

While democracy is the declaration of the mindset of free people, its Achilles tendon is that its decision-making process is significantly slower and more laborious than autocratic regimes because all matters are discussed many times by people not so relevant to the subjects under discussion. In the meantime, the adversary has the advantage of time and the element of surprise. Under that aspect, when it comes to national security matters, the decisions should be more **state-centered** by the core of experts in national foreign policy, intelligence operations, and internal policy for espionage, cyber threats to national assets, and infrastructure. An example of a state-centered decision-making process in the matters above is the Republic of France, a role model of democracy in Europe.

**Fast forward-moving world and compressed time of decision making with high impact consequences**

Real-time, parallel planning and decision making with more initiative to field operations leaders are where things tend to go, whether high-ranking officials favor it. The need is imminent to reinforce Human Intelligence (HUMINT) through long-term engagement in areas of future interest before intelligence becomes of high priority and is not available. Field Officers and low-ranking public and military service members should be required to make suggestions based on what they discover during on-ground operations and daily tasks, as they are attached to reality. This is a matter of developing leaders for already complex environments of decision-making. These people will have to make decisions during events that have a strategic impact and have no actual authority (Cal Speakers Series, 2018). Structures and Organizations need to have fewer layers of decision-making and approval to assist in this process. Having a lower rank in an agency does not mean being less intelligent, proactive, or wise. On the contrary, the younger generations are much more exposed to everything from a very early age because of the internet and the ability to travel a lot, which was not the case some decades ago. Good or bad, young people mature faster and can make decisions faster. Faster decision-making and unexpected situations are a growing trend. The nation that trains, trusts, and empowers its youth will ultimately prevail.

**Global organizations to solve global problems (Develop coalitions that promote partnerships and isolate non-participants)**

The U.S. cannot unilaterally face this emerging megatrend of having so many vital issues rising at the same time almost uncontrollably. The U.S. must communicate in a leading and persuasive manner that traditional organizations must reshape and proactively impose a solid strategy with no exemptions regarding climate change, the international legal framework for cyberwarfare and crimes, and introduce cyber security sanctions through global agreements. Moreover, there needs to be a clear understanding of the different perspectives that many countries in the Middle East and Africa see as “Western thinking and living.” For some, it is a threat and an enemy impersonated in the face of the U.S. There needs to be a combined, long-term information campaign to help those “enemies” of the western way of life, conveying that the west does not pose a threat, rather the ability of free expression, at the same time respect for the local, national, and cultural characteristics of nations. It is the first step to penetrating and making partners with skeptical nations. This can be achieved through **international, regional, state, local, and tribal intelligence cooperation and collaboration (collection, analysis, and dissemination).**

Totalitarian regimes must be faced with a different approach. How much of their population support do they have? How capable is the population of discarding their dictator? Diplomatic isolation and international sanctions have proven to cause significant harm to the population yet have nearly zero impact on the dictatorial regimes. Furthermore, spreading democracy should not be the flag of the west. **Changes cannot be imposed but instead provoked**.

**Strategic Competitors** China, Russia, and Iran have proven to be the central axis of competition and advocacy against the U.S. and the west. They also have one fundamental characteristic, which is their Achilles tendon. They have never had solid, long-term partnerships with anyone but rather alignments with one another under the scope of “the enemy of my enemy is my friend.” They should become enemies/rivalries between them.

**National Interests**

The endstate is addressing what is at risk for the U.S.

* First, it is the national character of the nation and the dividing tendencies that lead to an increase in extremism. What the next generation of Americans will remember this generation for should be the salvation of freedom, bravery, and unity.
* Second, the U.S. should be the leading nation in the global arena, leading the international effort to cope with climate change, cybercrime, and terrorism, unifying past adversaries, and supporting traditional allies and friends.
* Third concerns the kind of leaders that will lead through the challenges ensuring the continuity of policy implementation.
* Fourth is self-efficiency on quality food (ex. emphasize local bio-agriculture to secure food efficiency in the U.S. and thus create more working opportunities).

**Pressing challenges**

* Nation Unity U.S. reputation in areas of interest for economic development and partnerships.
* Border security,
* climate change, and disaster response.
* People’s ambiguous trust in their governments and faith in institutions.
* Building networks in failed states of U.S. interest where China and Russia have infiltrated.

**Institutions – Mechanisms - Legal Requirements**

The overwhelming public oversight for every matter, often led by non-subject matter experts, slows down procedures and puts obstacles by people that do not have the experience to offer solid counterarguments to what they are opposed to. Senior positions in the IC should be depoliticized. Their leaders warrant more than a simple political appointment; rather, each leader should be voted on by some element of the IC. Despite that, internal decisions should always be justified by facts. The **U.S.** **Constitution** safeguards the changes, and the changes derive from the spirit of the Constitution.

**Foreseeable Impediments**.

* The negative aspect of social media and press networks is that they serve foreign interests rather than national, spread fake news, and involve themselves with matters they have no expertise in.
* **On a government and corporate level,** theimpediments to any change are the lack of an adapting mindset for the “old guard” that will not step down for the younger to take over, greed, economy scale-based decisions, omitting the long-term effects of those decisions on the next generations (corporate greed) and the climate.
* Senior leaders lack the political will to make substantive, meaningful changes.

**CONCLUSION**

National Security and Intelligence are not simply about borders or spying on the enemy. They are initially about securing the inner part of the body (the Nation and Homeland) and then protecting it from threatening trends that the NSAct and the Intelligence Community should discover. Today’s world is all about networks. They form in geometrical progress and produce even more. Oversight authorities/committees should be confined to people who know the intelligence field and do not adhere to political manipulation. The U.S. must revise the spread of democracy doctrine as the statement for international engagements, recognizing that it does not appeal to every corner of the planet.

**References**

CAL Speaker Series. (2018). British Army Leadership: Developing our Leaders, Today and Tomorrow. Retrieved from <https://www.youtube.com/watch?v=zJ9htrevE0o>

Cohen a. Eliot, (2019), American Manpower Policy 1940-1970 in Citizens and Soldiers, The

Dilemmas of Military Service, Cornell Studies in Security Affairs, *Cornell University Press,* ISBN 150173377X, 9781501733772

Dunlap Jr., Charles J. (2011). Perspectives for Cyber Strategists on Law for Cyberwar. *Strategic Studies Quarterly* 5 (1): 81–99. **Error! Hyperlink reference not valid.**

Galeotti Mark. (2020). Transnational Organized Crime: Law Enforcement as a Global Battlespace in Bunker, Robert J., ed. 2002. Nonstate Threats and Future Wars. London: Taylor & Francis Group. Accessed October 5, 2021. ProQuest Ebook Central. <https://ebookcentral.proquest.com/lib/apus/detail.action?docID=1074648>

Hoffman Frank. (2007). Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington, Virginia <https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf>

Kesan P. Jay. (2011). Active self-defense strategy best deterrent against cyber-attacks. University Of Illinois At Urbana-Champaign, News Bureau. EurekAlert <https://www.eurekalert.org/news-releases/488861>

McChrystal, Stanley. (2011). It Takes a Network: The New Frontline of Modern Warfare, Foreign Policy, March/April. Accessed August 31, 2020. <https://foreignpolicy.com/2011/02/21/it-takes-a-network/>

National Security Act 1947, 50 USC Ch. 44: National Security from Title 50—War & National Defense

[https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter44 &edition=prelim](https://uscode.house.gov/view.xhtml?path=/prelim@title50/chapter44%20&edition=prelim)