|  |  |
| --- | --- |
| **How Can the U.S. Government and Private Enterprise Work Together to Reinvent Cybersecurity?**  *Here are some ways that you and your business can help* ***spark*** *much-needed change in the cybersecurity space.*  *This article was written in collaboration with Angelica Sirotin.*  Never before in our modern history have the issues of safety and security been more critical. The hot-button topic of cyber security vulnerabilities has mobilized a **fleet** of AI and technology entrepreneurs, who are **keen** of finding and implementing digital solutions to **avert** future crises while simultaneously mitigating current threats.  As a result of the latest chaotic developments in the US, a whopping 67 percent of small businesses aim to boost their cybersecurity in 2020. The only way to achieve this change is to leverage the power of American **ingenuity**, and reinvent our national security infrastructure through AI technologies that embody principles of ethics, transparence and accountability. Thankfully, a new era of cyber entrepreneurs is already here, fueled by global cybersecurity spending that is predicted to exceed $1 trillion from now until 2021.  **Arguably**, the quickest way to **disseminate** the message of cyber entrepreneurship and to provide lessons for the next gen of entrepreneurs is to hold critical dialogues that address such issues as national security.  After **conversing** with some of the best and brightest minds in national security, we came up with a list of best practices you can use in your business.   * **Support and leverage government policies.** It is important for private and public institutions to partner with government research labs to **garner** entrepreneurial **endeavors** and advance research into new, implementable cyber security strategies. * **Entrepreneurs become the core block of national resilience.** The U.S. 2017 National Security Strategy **relayed** the message that economic security is national security. The backbone of American ingenuity is one that national security frameworks depend on, as the public is the premise for safety and security protocols. * **Foster innovative ideas.** We must further mobilize entrepreneurs to continue innovating with leading AI technologies across sectors, and around the country, via the guidance of research institutions, private companies, and the government. * **Focus on human-machine interaction to bridge the gap.** Without trust between human-machine interaction, little can be done within the **realm** of progressing national security standards. According to a July 2020 report from *Research and Markets*, and based on evaluation from *The Baytown Sun,* “Machine-led automation systems alone are NOT enough to specifically understand the motives behind attacks as there is also a need for **cognitive** computing enabled human intervention.” As the future moves towards **convergence**, biology and technology must find a **common ground** with the aid of public-private intiatives, or future-proofing national security standards will result in failure. * **Gen Z should be more involved with entrepreneurship related to National Security.** Sometimes called the Surveillance Generation for having grown up alongside the internet era, social media, IoT, and the like – combined with the fact that Gen Z **is the most entrepreneurial generation yet**, this younger generation has first-hand knowledge of what the evolution of safety and security resembles. Moreover, according to the US Bureau of Labor Statistics, America requires “1.8 million additional cybersecurity professionals to fill the workforce gap by 2022.” This gap will be filled by Gen Z entering the workforce, and will have **profound effects** on our national security policies. Additionally, it is important to build off the previous experience of digital natives, and involve them throughout the reinvention of our national security protocols.   Finally, the experts we met with provided a call to action to U.S. citizens and entrepreneurs alike to stand up, innovate and reinvent cybersecurity frameworks in a way that reflects **resilience** and the spirit of this nation. | ***Spark:*** *to kindle, or stimulate.*  **Fleet:** the largest organization.  **Keen:** desire.  **Avert:** Prevent.  **Ingenuity:** the quality of being cleverly.  **Arguably:** được cho là, có thể nói rằng.  **Disseminate:** to spread widely / phổ biến.  **Conversing:** to talk informally with another or others.  **Garner:** thu hút.  **Endeavors:** make an effort, to attempt.  **Relayed:** truyền đi, gửi đi.  **Realm:** Lĩnh vực.  **Cognitive:** Nhận thức.  **Convergence:** Hội tụ.  **common ground:** Điểm chung.  **is the most entrepreneurial generation yet:** thế hệ có nhiều doanh nhân nhất.  **profound effects:** ảnh hưởng sâu sắc.  **Resilience**: ability to return to the original form, ability to recover. |