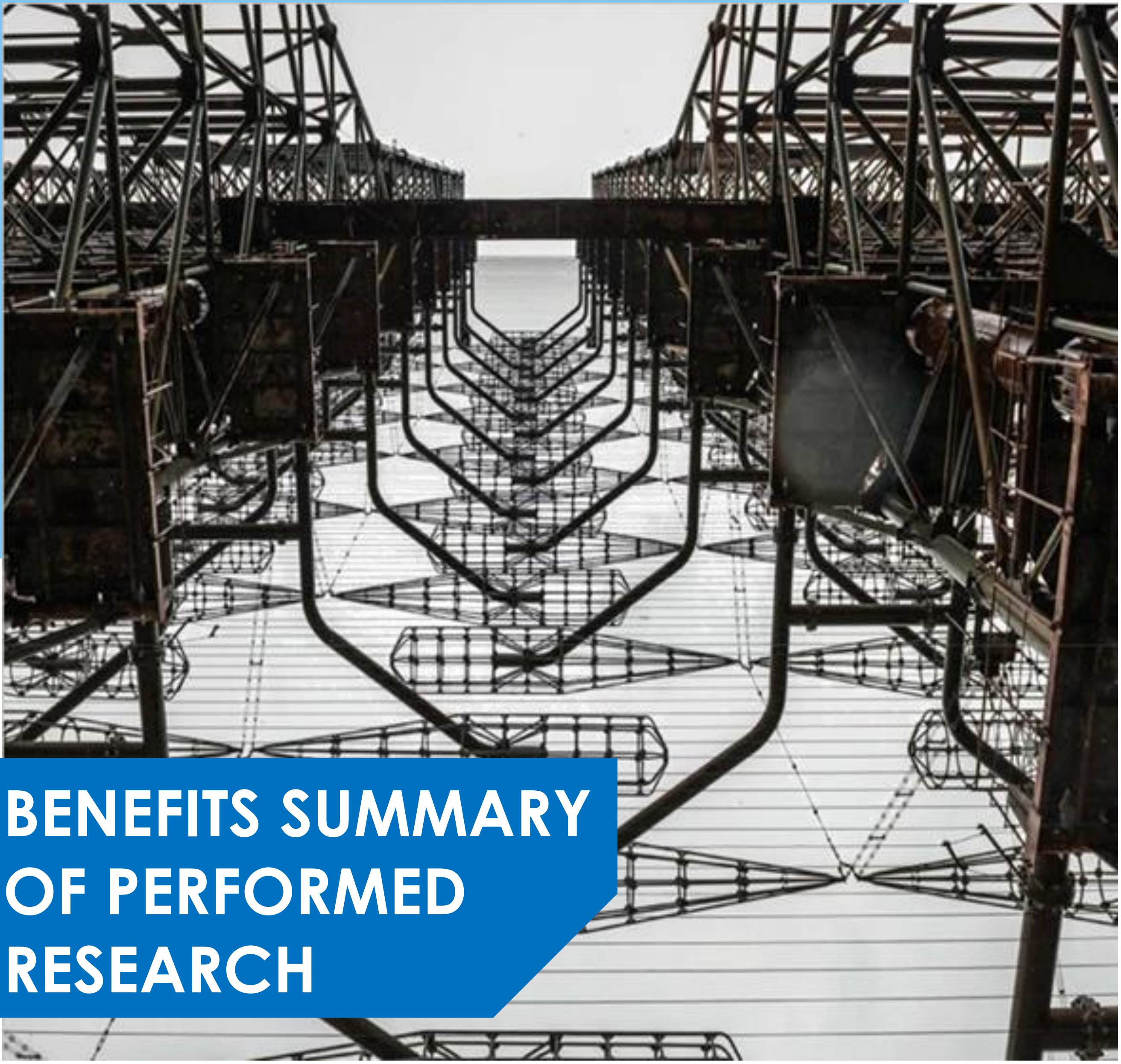

BENEFITS SUMMARY OF PERFORMED RESEARCH

Dr. Anil Lamba

Email: Dranillamba@outlook.com

Tel: [978] 674 9452

*According to the World Economic Forum's **Global Risk Report 2018**, which said: "**Cyberattacks are perceived as the global risk of highest concern to business leaders in advanced economies**. Cyber is also viewed by the wider risk community as the risk most likely to intensify in 2018, according to the risk perception survey that underpins the Global Risks Report."*

Advancing cybersecurity of Energy, Oil & Gas is a core priority for our country and needs immersed attention on this mission of protecting our most valuable assets, critical systems and networks. This report ensures effective, collaborative, enterprise-wide cybersecurity posture and defense.

Here are some key benefits of the research that CONTINUALLY IMPROVES CYBERSECURITY POSTURE of this National security concern -

- *This report helps analyze all critical types of cyber-security & information security attacks and provides an assurance to remediate **70% of all potential hacks** that could disrupt energy services and/or damage highly specialized equipment which is a key concern for human health and safety.*
- *This report presents a **4 step attack lifecycle** followed by hackers, highlights **16 specific cyber-security attacks** and its **recommended countermeasures** to focus remediation as governance efforts.*
- *This report helps recommend **technical suggestions** and enhance **guidelines for future's mandatory reliability standards** for energy systems.*
- *This report clearly articulates **challenges of cyber security** and provides **applied knowledge recommendations** for cyber-security preparedness, Incident Response and Resiliency of energy and Oil & Gas systems.*
- *Enhance **small organizational capabilities** to manage the cybersecurity risk and to **reduce the risk of energy disruptions** due to cyber incidents*
- *It helps to expand capabilities to **monitor, analyze, and share threat indicators**.*
- *Robust security requires monitoring and securing both enterprise IT environments and operational environments.*
- ***Strengthening of internal controls**, and standardization of processes and reporting to reduce the management complexity of cybersecurity functions.*
- *Augment the **foundation of cyber protection** & resilience in the core grid.*
- ***Provides a checklist to conduct assessments** to ensure that integration of new IT hardware, software, and firmware meet cybersecurity standards (along with legal and regulatory requirements) to prior to integration into the Department's information ecosystem.*
- *Develop and **implement an incident triage**, response, and recovery process to contain and eliminate cybersecurity threats.*
- *Define & Suggest controls technology to **improve reliability, security, and efficiency of the electric grid**.*
- ***Tightens policies and procedures** are in place to prevent intrusion and manipulation.*
- ***Combating targeted** phishing, denial of service attacks, and the introduction of malware into our systems.*

While the Whitepaper / Research outlines activities specifically for enhancing Cyber Security & Resiliency, the associated countermeasures and information will improve its posture and protect its systems, information, and infrastructure from the cybersecurity threat. This research will help to modernize IT infrastructure to deliver effective services that will support smart, efficient cybersecurity, increase resiliency, scale capacity and enhance cybersecurity risk management across the enterprise.