THE NEXUS BETWEEN CYBERSECURITY AND BIOSECURITY

WHITE PAPER

KEY INSIGHTS AND RECOMMENDATIONS FROM THE

WINNING THE PEACE SERIES

13 MAY 2020

HOSTED BY C5 CAPITAL

1701 PENNSYLVANIA AVE NW
WASHINGTON, DC 20006

SAVILE ROW HOUSE 7 VIGO STREET
LONDON W1S 3HF

This report is based on discussions that took place during the inaugural **Winning the Peace** discussion on Wednesday, May 13th. We virtually convened a talented group of over 80 technologists, military, government and industry leaders, including Gen. Jim Mattis, Bud MacFarlane, Adm. Mike Hewitt, Former Congressman Pat Tiberi, and Gen. Jim Keffer for a strategic discussion on **The Nexus Between Cybersecurity and Biosecurity**. All of our participants share a commitment to the US-UK alliance as a channel for preserving our sovereignty, security and prosperity toward a more resilient future. The event opened with remarks by André Pienaar, Founder and Chief Executive Officer of C5 Capital, sharing his prediction that the biosecurity sector will become as large as the cybersecurity sector in the near future. It was moderated by Sir Graeme Lamb, C5 Operating Partner & Former Director of UK Special Forces, and featured expert panelists Hamish de Bretton-Gordon, OBE RE(V) and Brigham B. Bechtel.

The Winning the Peace series is hosted by C5 Capital, a specialist venture capital firm. Throughout the series, our goal is to convene technologists, military, government and industry leaders to consider pillars of a post Covid-19 world order, rooted in the opportunity we consider for UK and US partnerships. Participant biographies can be found in Appendix 1. The participants were given the opportunity to comment on the draft final report, however its contents may only be attributed to the host rapporteur and do not necessarily represent the views or opinions of any organisation to which the participants belong.

C5 Capital is a mission-based venture capital firm investing exclusively in cyber security, artificial intelligence, cloud computing and space technology that advances national security for our country and our allies. C5 combines multiple verticals in its cyber investment strategy, including a substantial focus on the late stage/growth investments, an early stage venture capital accelerator and a broad network of operating partners, skilled in deep tech, to enable solutions to create value. This combination puts C5 in a differentiated class as the premier global firm with this mission-driven purpose. C5 creates its global reach from offices in London and Washington, DC.

C5 CAPITAL

1701 Pennsylvania Ave NW
Washington, DC 20006

Savile Row House 7 Vigo Street
London W1S 3HF
T: +44 (0) 20 3405 5300
E: enquiries@c5capital.com
W: http://c5capital.com

CONTENTS

EXECUTIVE SUMMARY

Until Covid-19 struck, pandemics and biological terror events were considered unlikely threats on the global scale. Yet today, we see biosecurity as a key global security concern that is cross-cutting with cybersecurity, geopolitical and economic risks. The US and UK must focus today on preparing for the next pandemic or biological terror event to ensure our collective physical and economic resilience. Like any threat, with the appropriate mitigations in place, up front, governments can ensure the required resilience to mitigate potential human and economic costs.

A Covid-19 scale event was hitherto considered to be a 1 in a 100-year event. Across the last century of Spanish Flu, MERS, SARS and EBOLA outbreaks, experts now realise that biological threats should be expected to become more frequent. With global travel norms such that at any given moment, over a half a million people are in the air, we know that infectious disease can traverse the globe in 24 hours. Over the last 30 years, the number of 'Level Four' biological facilities worldwide has grown to 70. These are the facilities where the most dangerous pathogens are being stored and studied. As part of our evolving biosecurity strategy, we should consider trends of increasing global connectivity and viral propagation as signs of a growing threat vector for greater scrutiny.

From a strategic perspective, we should focus our attention on biosecurity strategy from the counter-terrorism angle given that biological weapons have the potential for massive psychological and despiriting impacts on citizens. The fear factor to the public is 10 to 1 relative to that of kinetic attacks. The cornerstone to an effective strategy should also cover preparation of a huge volume of factual information to countervail the tsunami of disinformation and propaganda expected in any biosecurity event.

Mitigation for Resilience

Ensuring resilience requires a three-pronged approach to address the following:

- **Data –** Biosecurity measures will require the collection, sharing, and securing of vast amounts of data. As we use this information to secure our future, the confluence between biosecurity, economic growth and systemic financial stability cannot be understated.
- **Medical Countermeasure (MCM) development** – This is the silver bullet. Medical countermeasures (MCMs) are products such as biologics and pharmaceutical drugs that can protect from or treat the effects of a pandemic or biological attack.
- **Domestic production of MCM & PPE** – Domestic supply and manufacture is required. We must avoid increasing our reliance on China for PPE and MCM in future.

In order to have an effective biosecurity stance, the US and UK should work together closely as permanent members of the UN Security Council. It is highly likely that China and Russia will veto measures to broaden the Biological Weapons Convention and other controlling protocols. The 'silver bullet' may lie in medical countermeasure development, where these two countries are the world leaders. Increased domestic production of MCM, ventilators, and personal protective equipment (PPE) is essential to avoid outsized reliance on China for critical supplies in future. A shared responsibility between the US and UK to produce critical healthcare inputs may be the most effective way to shore up supply chain security. Strong data governance, ensuring credibility, security and access to shared information, and robust democratic leadership are all essential to delivering a viable and effective biosecurity road map in future.

China has many questions to be answered and must be held to account.

FOREWORD FROM HAMISH DE BRETTON-GORDON AND BRIGHAM B. BECHTEL

on Friday, May 15th, 2020

Biosecurity, as originally conceptualized, was a set of preventive measures designed to reduce the risk of transmission of infectious diseases in crops and livestock, quarantined pests and living modified organisms. From the 1990s, in response to the threat of biological terrorism, biosecurity began encompassing the prevention of the theft of biological materials from research laboratories. The emerging nature of biosecurity threats shows that small-scale risks can propagate rapidly across the globe. Designing effective policy becomes a challenge for there are limitations on time and resources available for analysing threats and estimating the likelihood of their occurrence.

The term biosecurity now includes the management of biological threats to people, industries or environment, and extends to **pandemic diseases** and the threat of **bioterrorism**. The World Health Organisation provided an information note describing biosecurity as a strategic and integrated approach to analysing and managing relevant risks to human, animal and plant life and health and associated risks for the environment.

Advances in technology have meant that many civilian research projects in medicine have the potential to be used in military applications ('dual-use' research) and biosecurity protocols are used to prevent dangerous biological materials from falling into the hands of malevolent parties. Controversial experiments in synthetic biology, including the synthesis of poliovirus from its genetic sequence, and the modification of H5N1 for airborne transmission in mammals, led to calls for tighter controls on the materials and information used to perform similar feats. There are now over 70 level 4 containment facilities worldwide where the most potent pathogens are stored and worked on. This is a massive increase over the last 30 years. We see this prevalence as an Achilles heel that now requires much greater control and oversight, as part of a **global biosecurity defence network.**

As we face an increasingly uncertain future, with renewed awareness of our societies' biological vulnerabilities, we must consider how to strengthen our bio-resilience. This can be achieved through robust investment in healthcare systems, the preservation of biodiversity and mitigation of ecological disruptions. Government investments in social infrastructure to reduce the spread in health indicators across sociological and demographic lines can be powerful tools in this arena. To succeed, all of these measures will require the collection, sharing, and securing of vast amounts of data. As we use this information to secure our future the confluence between biosecurity, economic growth and systemic financial stability cannot be understated.

Thank you for joining us in the conversation.

Hamish de Bretton-Gordon, OBE RE(V) &
Brigham B. Bechtel

I. The Race Between Time and Knowledge

> *Grappling with the Covid-19 pandemic, we are struck with the human cost of the passage of **time**, as we pursue the **knowledge** necessary to find life-preserving technologies. Time and knowledge cannot be outpaced. We need to de-code the virus, re-code a vaccine, and contain it through tracking, testing and tracing before we can hope to control it. Each of these endeavors requires massive volumes of data - which must be available, shared and secure at all times. Data is the bridge between cybersecurity and biosecurity.*

Data systems and pandemics have one thing in common: they never sleep. A satellite 22,000 miles above us can transmit data to our cellphones in nanoseconds. Infectious disease can traverse the globe in 24 hours. How do we see the control and use of data as key to preventing and subsequently managing a pandemic, or biological attack response?

The protection and prevention of manipulation of that data is sacrosanct. Case in point: The loss of at least seven days of data and dis-information following the initial Covid-19 cases identified in Wuhan allowed the virus seven days to spread unchecked, and it did so globally. Countries such as New Zealand with relatively strong data governance were able to leverage early insights from widespread testing data into early, and decisive public policy action. New Zealand thereby significantly reduced the impact of the virus on their population and the prime minister of New Zealand, Jacinda Ardern has since been named Most Effective Leader on the Planet.[1]

As governments and citizens focus an ever increasing share of their attention on Covid-19, we find ourselves in a fog of attention fatigue and anxiety that ultimately amplifies our cyber vulnerability. Hackers approach this fog opportunistically. We have observed a ten-fold increase in cyberattacks such as ransomware against the healthcare sector since March, adding additional threat to already-overburdened hospitals, clinics and research facilities. Similarly, the World Health Organization (WHO) recently warned that over 25,000 email addresses from its organisation and others related to its operations – such as the UK's National Health Service (NHS) and the National Institutes of Health (NIH) in the US – had been compromised.

There are two interlocking trends driving the increased threat. First, as businesses and organisations across the world move more of their operations online and enable remote work, the attack surface widens dramatically. Second, the financial opportunity structures around cyber crime have shifted. The pandemic has created an overnight, multi-billion dollar industry for therapeutics. Cyber criminals, whether state or non state actors, are incentivised to steal intellectual property or halt critical healthcare operations using ransomware to elicit financial gains.

The enablement of mobile tracking, testing and tracing required to contain Covid-19 transmission must address Bluetooth vulnerabilities, employ security technologies such as AI-powered behavioural network analytics, homomorphic encryption, and sound processes to ensure the integrity of observed data.

---

[1] Friedman, Uri (2020), "New Zealand's Prime Minister May Be the Most Effective Leader on the Planet", *The Atlantic*, 19 April.

II. Availability Bias and the Paradigm of Danger vs. Uncertainty

> *Thucydides, a 5th century BC Athenian general in Athens during the outbreak of the plague once wrote, "For the catastrophe was so overwhelming that men, not knowing what would happen next to them, became indifferent to every rule of religion and of law". This quote brings into sharp relief how dangerous fear is to social stability. Thomas Schelling, a 20th century American economist and professor of foreign policy, national security, nuclear strategy once described "the essence of the crisis is its unpredictability. The 'crisis' that involves no risk of things getting out of hand is no crisis — It is the essence of a crisis that the participants are not fully in control of events". This pandemic, while we struggle to understand it, creates the conditions for 'persistent uncertainty', and uncertainty swells our assessment of the real danger at hand.*

Facts and expertise are under fire. Hamish recalled the site of a barrel bomb impacting a hospital in Aleppo. He implored his colleagues to help rescue victims inside the hospital and storm in. The fear of potentially dangerous nerve agents in the facility paralysed all from action. Hamish recalled that he was taken aback by the impact of fear and the perception of certain danger to paralyse them from action. Their response: We can hide from bombs and bullets, but we can't hide from gas. At the same time, the chances of germ warfare being used on the battlefield are, by any historical measure of incidence - slim.

The paradox is thus: access to full and complete information may prevent fear from perpetuating.

The need for mass reassurance about the uncertain future we face has created a marked increase in media appetites. This leaves our citizens open to the bombardment of misinformation at their doorsteps. Broadly circulated disinformation about the Covid-19 pandemic has engendered huge amounts of fear and public distrust. The willingness for populations to go back outside to public places will depend to a large degree on their perception of the danger, which in turn is based on media diets. Increased government action to combat the spread of dis-information and repeat good information will give people confidence to go back out in public places and normalise economic activity, once shelter in place orders have been lifted.

At times, our governments have a difficult time circulating good information because we must be immutably accurate, and measured. Russia and China are not bound by the same constraints, and may utilise voids created by Western silence to transmute dis-information. Non-democratic nation states play at a relative advantage in the area of dis-information campaigns. All that it takes for an adversary to lead a successful campaign to deflect, disrupt, distract, and destroy our citizens, is their willingness to listen. Dis-information campaigns arising from biological events are a real threat to our democratic societies. Consider the Salisbury nerve agent attack as it served a massive advertisement to global dictators, despots, rogue states and terrorists on the potential impacts gained from chemical attacks. Covid-19 has done the same for the global perception of biological attacks or pandemics.

III. Spirit of the Atlantic Charter at a Crossroads

> *The Atlantic Charter was founded on an alliance of a community of nations, of a united belief, of spirit, interests and common thought symptoms can be dealt with nationally but to address the cause will demand Allies and Alliances of International standing to deal with it, joining forces to face a common enemy.*

As Bill Gates has recently stated, we are in a world war, only all of humanity is on the same side. Effective alliances are built not just out of necessity, but trust. Current global and national politics are not defined by an overabundance of trust, but deal with a lack of mutually trusted institutions, unwillingness to share relevant data and political polarisation of unique proportions. We hold this as evident given that the threat analysis of Covid-19 itself has become a partisan issue around the world, informed to a degree by fake news and political opportunism.

When US and UK governments joined forces, the degree of intelligence and resource-sharing represented a first in modern nation-state history. Rarely before were two nations willing to reveal their capabilities, covert information and strategies to one another, but the common enemy they faced didn't permit politics as usual. One can only imagine the opportunities lost if they spent time blaming each other over failed missions, attempted to out compete one another over military might, or siloed critical intelligence into their respective domains. Enumerating the opportunity costs of nationalism in the context of this pandemic brings us to the realisation of what is truly at stake.

The coronavirus, as a mass threat, is exactly the type of enemy that can be best fought united. Each individual country holds the potential set of data, or insight or research that could be the key in finding the right public policy or even a vaccine. While academic cooperation has remained very strong, political cooperation should be the defining factor to save lives.

The same type of best-practice and data exchange will not only help to overcome the virus, but also define the success of restarting the global economy. How effective any one nation is at halting the spread is no guarantee for overcoming economic pains. While global cooperation is essential to beat Covid-19, it is also key to generating growth, jobs and stability.

It is that very understanding and mentality, that statesmen and women have understood in 1941, that not one nation or one army or one politician would end fascism, but a joint effort of like-minded people, unburdened by trying to win the moment, focused on winning the peace.

Appendix 1. Participant Biographies

HOST: **André Pienaar, CEO and Founder, C5 Capital**

André Pienaar is a Managing Partner and the Founder of C5. André serves on the boards of IronNet Cybersecurity in Maryland, USA, the Haven Group in Luxembourg and ITC Secure in London. He previously served on the Boards of Omada, Balabit and Shape Security which C5 exited successfully.

André started his career at Kroll Inc in 1996 where he became the youngest managing director until the successful sale of the company to Marsh & McLennan. In 2004, André went on to found G3, an international consulting firm that advises global companies and international law firms on cybersecurity. In 2011, he sold G3 to Europe's leading technology investment holding company. André advised the 6th Duke of Westminster on the establishment of the new Defence and National Rehabilitation Centre (DNRC) in the United Kingdom as a state of the art centre for the rehabilitation of British military veterans. André is a lawyer and an expert on cyber law and cybercrime.

MODERATOR: **Sir Graeme Lamb, Operating Partner, C5 Capital & Former Director, UK Special Forces**

Lt. Gen. Sir Graeme Lamb has had a long and distinguished military career with both the Regular and UK Special Forces, of which he was Director from 2001-2003. Sir Graeme has been formally recognised by Her Majesty's Government seven times for his service to the nation.

PANELISTS: **Hamish de Bretton-Gordon, Leading Biological Security Expert**
Hamish de Bretton-Gordon is a world leading expert in Chemical and Biological weapons. He is also a director of the NGO 'Doctors Under Fire' and an advisor to the Syrian Medical charity UOSSM. Hamish is a commissioned reserve officer in the Army's Engineer & Logistic Staff Corp as senior advisor & mentor to the MOD on CBRN.

Hamish served 23 years in the British Army including service as Commanding Officer of the UK CBRN Regiment and NATO's Rapid Reaction CBRN Battalion. His operational deployments included the 1st Gulf War, Cyprus, Bosnia, Kosovo, Iraq and Afghanistan and has been in Syria & Iraq frequently in the last 8 years. This considerable experience in the field places Hamish as one of the world's leading and most current experts in chemical and biological counter terrorism and warfare, and in 2005 he was appointed an OBE for his exceptional performance.

Hamish on leaving the Army in 2011 founded the biosecurity company SecureBio. This company was acquired by Avon protection in 2014 where Hamish was a senior executive until April 2020. He has worked with the

Kurdistan Regional Government in Northern Iraq to decontaminate Halabja, and has most recently provided guidance to civilians, UK Government and the international community on safety round chemical and biological weapon use in Syria and Iraq. Hamish has worked in Syria during the current conflict setting up the CBRN Task Force and advising medical charities, the White Helmets and the Idlib Health Directorate on treating the victims of chemical weapons attacks and collation of evidence. He advised the Peshmerga 2015-17 on CBRN matters and trained them on a number of occasions to counter the ISIL chemical attacks in N. Iraq. Hamish is probably the leading expert on ISIS CBRN capabilities and plans and was 'gassed' by them near Mosul in April 2016. He travels regularly to the US, Syria, Iraq and other Middle and Far Eastern countries advising on CBRN Counter Terrorism and humanitarian support in warzones. He lectures on CBRN and humanitarian intervention at Cambridge, Imperial and Bournemouth Universities.

Today, Hamish gives advice to UK Government agencies and is a senior MOD advisor on CBRN and Syria, and is frequently seen on global news channels providing expert commentary, and writes in UK, Middle East and US news journals and newspapers. He takes up the position of Distinguished Visiting Fellow at Magdalene College Cambridge this October, and his memoir 'Chemical Warrior' will be published on September 3rd, 2020. Find out more here: https://t.co/Q4xfIBMhJA.

Brigham B. Bechtel, Leading Security Expert

Brigham B. Bechtel is a 31 year veteran of the United States intelligence community, having served for more than 26 years in the Central Intelligence Agency with experience in leading operations and analysis in South Asia, West Africa, and the Middle East. Mr. Bechtel formerly led crisis response elements and served with the FBI Chemical/Biological/Radiological-Nuclear Weapons Investigation Unit. He spent six years in analysis, and authored publications on conventional military forces, WMD and terrorism. He was the lead analyst supporting counter-terrorist operations in Central Europe from 1997-1999. Mr. Bechtel began his career in the intelligence community as a Cryptologic Technician in the United States Navy before joining the CIA. Mr. Bechtel is a Truman Scholar from the State of Maryland for 1987; he is a 1989 graduate of St. John's College of Annapolis, Maryland.