SAFEGUARDING BUSINESS AND NATIONAL INFRASTRUCTURE

Views from J.P. Morgan's International Council

INTRODUCTION

Strengthening cybersecurity is an increasingly urgent challenge for business and political leaders alike, one that requires fresh thinking and sustained attention from all levels of government and society. Cyber attacks in 2021 grew in number and sophistication, demonstrating that both state actors with vast resources as well as criminal groups have the capacity to threaten critical infrastructure and ultimately national security. Developing more effective defenses against cyberattacks requires shared commitment and close collaboration between the public and private sectors.

The J.P. Morgan International Council, a group of CEOs and former senior policymakers from across the globe, gathered virtually and in person throughout 2021 to discuss how government and business can better work together to confront the cybersecurity challenge. Participants included former Prime Minister Tony Blair; CEOs Jamie Dimon (JPMorgan Chase), Alex Gorsky (Johnson & Johnson), and Aliko Dangote (Dangote Group); former Secretaries of State Condoleezza Rice and Henry Kissinger; and former Secretary of Defense Robert Gates. Throughout the discussions, the Council was advised by former Under Secretary of Defense for Policy and Managing Partner of WestExec Advisors, Michèle Flournoy.

Council members recognized the enormous amount of work underway in both the U.S. Congress and the Biden Administration to tackle this massive challenge. The Council also saw opportunities to amplify these efforts, while pointing to new areas for public policy action, including the following:

Strengthen Collaboration Between the Public and Private Sectors by:

a. Boosting Capacity of Government and Business
b. Sharing Timely Information
c. Promoting Accountability

Turn Policy Into Law by:

Passing legislation to codify key provisions of E.O.s. enacted under current and prior administrations

Elevate International Cyber Diplomacy by:

Intensifying diplomatic efforts among like-minded countries to enhance intelligence sharing, encouraging public-private collaboration at the international level and defining and enforcing norms of cyber behavior

Cyber is the most dangerous weapon in the world—politically, economically, and militarily. The public and private sectors must work together to fortify our business and government activities against this threat, and adequately educate the American people about just how dangerous this weapon is.

Robert Gates ■ *Former U.S. Secretary of Defense and Vice Chairman of the J.P. Morgan International Council*

1. STRENGTHEN COLLABORATION BETWEEN THE PUBLIC AND PRIVATE SECTORS

Unlike in other forms of warfare, in cyber the private sector is often the front line, which means that communication and collaboration between government and business needs to be equal and two-directional. Members of the Council took note of the important progress being made in improving public-private cooperation but also identified the following three areas for further work.

a. Increase Technical Capacity of Government and Business

In the U.S., the government and private sector have collaborated to address cyber risk for two decades. Roles and responsibilities are still being defined in the collaborative model, but some lessons have emerged clearly. The Council recommends working with and integrating existing successful models and not spending scarce resources on developing new models from scratch. Council members view sector-based approaches to public-private cooperation as best suited to address cyber threats effectively. These approaches build on existing contacts between industry sectors and their government regulators or partners. Government should use its influence to encourage the development of private sector entities designed to support both government and private sector missions. Such an approach, particularly in the finance sector through the Financial Sector-Information Sharing and Analysis Center and the Analysis and Resiliency Center, has been successful to date. Public-private participants can all benefit from the output of these organizations' work, without needing to duplicate efforts and cannibalize the limited personnel qualified to support such efforts.

Expertise related to the business and technology operations of specific sectors is of primary importance. The government—from federal down to local levels—must hire more cyber experts and must ensure that all relevant departments and agencies have them. The ability of federal government agencies to manage relationships with businesses effectively across a variety of sectors greatly depends on the level of technical knowledge in each agency. In some cases, the government agencies and departments to which certain sectors will turn for help have little or no cyber expertise—for example, the Department of Health and Human Services for the entire health care system or the Department of Agriculture for food supply chains. Without such expertise, government agencies will be unable to make sense of the risk analyses that companies produce.

State and local governments often have even less technical knowledge. The Cybersecurity and Infrastructure Security Agency (CISA), charged with leading the defense of key critical infrastructure, is receiving more resources to invest in staff. CISA needs to work with government agencies on an urgent basis to help build their expertise and, in the meantime, connect key offices in those agencies directly with CISA for quick referral and help for companies in sectors they oversee. However, most of the funds that continue to be allocated are going to reinforcing the defenses of federal systems, while funds dedicated to private sector collaboration are a small fraction of CISA's overall budget. More funding is needed to address this shortfall as the newly bolstered CISA finds its footing.

Cyber risk is of critical importance to countries, economies, and businesses. To help protect national security and overcome impediments to trade, we need to hold bad actors accountable, provide transparency to those affected by incidents, invest in the uplift to cybersecurity, and adopt safe and sound practices for data protection and handling.

Jamie Dimon ▪ *Chairman of the Board and Chief Executive Officer, JPMorgan Chase & Co.*

Council members see a need to boost cybersecurity capacity of small- and medium-sized enterprises (SMEs), particularly because they are sources of vulnerability for large firms. SMEs typically lack the resources and expertise of larger firms to defend themselves, while cyberattacks against them pose risks not only to the SMEs but to larger firms doing business with them and to supply chains reliant on them. SMEs pose risks to national security given how tightly knit U.S. global supply chains are. Larger firms must do more to partner with and mentor SME clients, suppliers, and vendors in addressing cyber threats. Council members urged the government to help here, as well, by offering positive incentives and negative consequences to encourage best practices through grant programs, subsidies, and tax breaks.

b. Improve Information Sharing

Council members encouraged the government to share more information on cyber threats and to do so in a more timely fashion. After Colonial Pipeline and SolarWinds, it's obvious to both government and industry that more needs to be done around information sharing and incident notification, but there is a perception among some business leaders that the government is not sharing as much information as it could, which undermines trust and discourages businesses from sharing information in kind. To be effective, government should fill gaps where there is no private sector alternative (i.e., by sharing unique intelligence) or seek to stimulate markets that it believes are not well served (i.e., SMEs) through grant funding or other programs. SMEs, most of which have little to no regular direct engagement with federal authorities, may not know immediately to which agency to turn in the event of threats and attacks without more consistent information sharing.

CISA is now working to address this issue by establishing more "operational collaboration" through the Joint Cyber Defense Collaborative (JCDC), which was established in late summer 2021. Though members of the Council applauded the undertaking, the JCDC is a nascent effort and will require effective implementation and execution. The JCDC is slowly scaling up to take on a greater number of private sector participants, including the financial sector in 2022. The Council urges CISA's JCDC to establish contact urgently in all 16 critical sectors, if for no other purpose than to inform trade/industry associations and companies in those sectors about the threat, the importance of information sharing, and whom to call for help. As JCDC expands further, a demonstrated track record of success will be essential in boosting private sector participation, which is entirely voluntary at this stage.

c. Promote Accountability

The Council endorses U.S. government efforts to define and enforce minimum standards of cybersecurity for critical infrastructure as envisioned in Executive Order (E.O.) 14028 and recommends that policy continue to encompass a broader and broader swath of the private sector. The government should also advise companies on metrics, through something like the proposed Bureau of Cybersecurity Statistics, that could be used by CEOs and Boards to assess and test their cyber defenses.

Council members also encouraged governments to do more to hold cyber criminals accountable. Some businesses, particularly in the technology sector, remain reluctant to share sensitive commercial data with the government to strengthen cybersecurity, fearing that government officials could mishandle the information in ways that would hurt their bottom line and competitive position. In this new world, however, businesses must be willing and able to share weakness in order to strengthen the entire system. In doing so, they can lead the cyber response. The Council was clear that ensuring cybercriminals are brought to justice in a more timely manner would build greater trust and improve information sharing. Doing so would also help inform the public of the serious nature of the threat, which Council members worried has not been fully appreciated to date. The recent arrests of cybercriminals associated with the REvil hacker group by U.S. and European authorities, accompanied by concurrent steps by the U.S. Treasury intended to disrupt future attacks, were clear positive steps forward and a roadmap for the future.

2. TURN POLICY INTO LAW

Given broad bipartisan support in the U.S. Congress for enhancing cybersecurity, members of the Council called for the White House and Congress to work together to pass legislation to codify key provisions of E.O.s. enacted under current and prior administrations.

The Biden Administration and Congress should capitalize on a rare moment of bipartisan agreement on the seriousness of cyber threats and turn relevant Executive Orders into law.

Condoleezza Rice ▪ *66th U.S. Secretary of State*

Members of the Council acknowledged that the Biden Administration has made important strides in addressing longstanding shortcomings in the federal government's approach to cybersecurity, particularly through its enactment of E.O. 14028 in May 2021 and the creation by Congress and appointment of a National Cyber Director at the White House. The detailed E.O. emerged in the aftermath of a number of high-profile cyberattacks against the government and private industry, including most notably the SolarWinds hack. Among other things, it called for enhancing government capabilities and collaboration, identifying minimum standards of security for industry, and improving data sharing. As of this writing, the E.O. has largely been implemented and should improve the U.S. government's ability to defend and respond to cyberattacks. This E.O. built on E.O. 13636 from the Obama Administration, which sought to boost critical infrastructure cybersecurity.

Council members recognized that E.O.s as policy tools provide a powerful and quick means of addressing pressing issues but noted that all E.O.s can be easily overturned by subsequent administrations. Failure to turn E.O.s into law with appropriate resourcing risks undermining nascent, overdue progress and increases risks to commercial activity and national security. The Council would therefore strongly support efforts by the Administration and those in Congress to adopt legislation to codify and support cybersecurity E.O.s.

3. ELEVATE INTERNATIONAL DIPLOMACY

Council members saw a need for more intensive diplomatic efforts among like-minded countries to enhance intelligence sharing, encourage public-private collaboration at the international level, and, perhaps most critically, define and enforce norms of cyber behavior.

There are a number of international bodies addressing cyber threats, including the G7, NATO, the Quadrilateral Security Dialogue, and others. Each has its own comparative advantages, but members of the Council believed that these efforts should be elevated in priority. Launched in 2018 by French President Macron, the Paris Call for Trust and Security in Cyberspace, or simply the Paris Call, has attempted to tie these various efforts together and has developed a set of nine principles to secure cyberspace. Eighty countries have signed on thus far, including the United States, as has the European Union. The Paris Call principles attempt to codify laudable norms of behavior, including protecting critical infrastructure and the integrity of free elections, but must be seen as a starting point because they lack governing structures or enforcement mechanisms.

The United States and its allies must build upon the work of the Paris Call and the lessons from the field of arms control to engage Russia and China in discussions on what constitutes unacceptable state-sanctioned or state-tolerated behavior in the cyber arena. The aim of such talks would be to take certain types of cyberattacks, such as those directed at certain types of critical infrastructure, off the table. Accountability for violations would need to be multilateral and carefully calibrated to avoid unintended consequences. To help spearhead this effort, Congress should support the Cyber Diplomacy Act aimed at establishing the Bureau of International Cyberspace Policy within the Department of State by confirming an ambassador to lead the group.

To confront growing concerns around cybersecurity, the international community needs to redouble efforts to develop common standards, establish and enforce norms, and coordinate responses to future cyber threats.

Tony Blair ■ *Former Prime Minister of Great Britain and Northern Ireland and Chairman of the J.P. Morgan International Council*

CONCLUSION

The cybersecurity threat is set to grow in intensity and scale for the foreseeable future. As the U.S. government, along with its allies, takes needed steps to address the threat, governments and businesses should continue to find ways to work more closely together. To help these efforts, members of the Council will engage senior policymakers and lawmakers to applaud progress where warranted and draw attention to the above areas for improvement.

About the International Council

Meeting for the first time in 1967, the International Council was founded to address the rapid expansion of J.P. Morgan's business outside of the United States. At that time, the firm's chairman and president perceived a need for an advisory group whose stature and experience could help to better understand key global trends. Since its inception, the Council has provided valuable insights and been instrumental to the development of the firm's strategy and outlook. Former Prime Minister of Great Britain and Northern Ireland Tony Blair serves as the Chairman, and former U.S. Secretary of Defense Bob Gates serves as the Vice Chairman. Other members include the Chief Executive Officers and Chairman of international corporations including Siemens AG, adidas, Johnson & Johnson, Alibaba Group, Tata Sons Ltd, and Saudi Aramco.

Over the years, the Council has provided the firm with the diverse perspectives needed to develop the most innovative solutions for our clients. Each year, we bring together these leaders in business and public service to discuss the major issues affecting the economic and geopolitical landscape. We believe that periodic consultation with such a group provides the firm and its clients with unparalleled knowledge and experience from their respective regions and local markets and is of great mutual benefit to both participants and the firm.

Acknowledgements

We are grateful to our partners at WestExec Advisors, Energy Futures Initiative, Council on Foreign Relations, Atlantic Council, Global Counsel, and the Tony Blair Institute for Global Change for their advice and support in shaping and facilitating these discussions.