Cyber Risk In A New Era: How Cyber Risk Affects Sovereigns

October 31, 2022

Key Takeaways

- The direct impact of cyber attacks for sovereign ratings will likely remain limited.
- The growing sophistication of attacks and digitalization of government operations and services could increase financial costs for governments from a successful attack.
- Sovereigns with weaker governance and institutions, and less robust fiscal and external accounts are probably less prepared for cyber risks, and therefore more likely to be impacted.
- Cyber attacks motivated by geopolitics could be more costly and impactful for a sovereign, in our view. Governments should therefore consider increasing investment and spending to create robust IT systems and back-ups.

PRIMARY CREDIT ANALYST

Zahabia S Gupta
Dubai
(971) 4-372-7154
zahabia.gupta
@spglobal.com

SECONDARY CONTACTS

Roberto H Sifon-arevalo
New York
+ 1 (212) 438 7358
roberto.sifon-arevalo
@spglobal.com

Dhruv Roy
Dubai
+ 971(0)56 413 3480
dhruv.roy
@spglobal.com

Valerie Montmaur
Paris
+ 33144207375
valerie.montmaur
@spglobal.com

Christian Esters, CFA
Frankfurt
+ 49 693 399 9262
christian.esters
@spglobal.com

Martin J Whitworth
London
+44 2071766745
martin.whitworth
@spglobal.com

See complete contact list at end of article.

We expect governments to face rising exposure to cyber attacks due to growing digitalization across government operations and services and the critical role played by a sovereign in providing public services and infrastructure. The effect of a cyber event on a sovereign rating will depend on the target, scope, and consequences of the attack. It could affect a sovereign rating if it had a material impact on one or more of the five sovereign rating factors in our sovereign criteria (see table 2).

Cyber attacks have become a key element of geopolitics, involving state and non-state actors. Attacks on Iran's nuclear facilities via a computer worm called Stuxnet more than a decade ago demonstrated how cyber capabilities can be used to achieve cross-border and physical damage. As we've seen more recently in the Russia-Ukraine conflict, cyber attacks can precede or accompany military action as part of hybrid warfare, with key targets being a country's critical infrastructure or services. In cases of imminent or rapidly rising external or internal political risk, (such as war, escalating domestic conflict, or acute and growing risk to institutional stability), S&P Global Ratings could lower the indicative sovereign rating on the basis of event risk, depending on the conflict's expected magnitude and effect on the sovereign's credit characteristics.

Although we believe that the scale and financial cost of cyber attacks will likely increase, we currently anticipate limited impact for sovereign ratings. Sovereigns--relative to other asset classes such as corporates or financial institutions--often benefit from a large and diverse economic and revenue base, substantial financial and non-financial resources, and flexibility to

raise additional revenue, which should limit the potential impact of cyber incidents.

That said, sovereigns with weaker governance, less diversified economies or revenue sources, and facing high geopolitical risks are likely to be more susceptible to negative impacts from cyber attacks.

Why Sovereigns Are Attractive Targets For Cyber Attacks

Sovereigns play a key role as a provider of public goods and services and regulations. They collect and process confidential identification, health, pension, and other sensitive data at the national level, much of which is increasingly digitized. The COVID-19 pandemic has accelerated the digital transformation of government processes, operations, and services. This has increased efficiency in many instances, but also makes them more susceptible to cyber attacks that could be driven by criminal intent.

Moreover, cyber attacks have become a prevalent means to achieve foreign policy objectives. That reflects their low deployment costs relative to conventional military tactics, difficulties in attribution, and uncertainty surrounding the scope for retaliation. We are also seeing a hybrid, cyber-kinetic form of warfare, where cyber assaults can precede or be accompanied by more traditional military operations. The intent of such attacks is often to undermine confidence in key institutions and infrastructure, which implies wider credit implications across sectors and geographies.

It can be problematic to trace and attribute cyber attacks, which makes them an attractive mechanism to target sovereigns while limiting retribution. States can choose to hide behind non-state proxies by encouraging nationalistic or sympathetic groups to implement their agenda.

The table below outlines some key motivations and outcomes of cyber attacks on sovereigns.

Table 1

Motivation Typically Dictates Sovereign Cyber Attack Taxonomy

Motivation	Foreign policy goal	Political agenda	Access to data or government resources
Means	Espionage, influencing elections, regime change, hybrid warfare (cyber and kinetic tactics).	Promotion of social, political, or ideological agendas, for example through propaganda, misinformation campaigns, or defacement of government websites.	Accessing sensitive information, including national identification details, social security data, tax data, and personal addresses for blackmail or sale.
Actors	State, state-associated or sympathetic non-state groups	Largely non-state domestic or international groups, including online activists	Financially motivated criminal groups.
Typical types of attacks	• Malware attacks • Distributed Denial-of-Service (DDoS) attacks • Sabotage or disruption of critical infrastructure/ services • Misinformation and misdirection	• DDoS • Malware attacks • Misinformation and misdirection	• DDoS • Malware attacks • Ransomware

Table 1

Motivation Typically Dictates Sovereign Cyber Attack Taxonomy (cont.)

Motivation	Foreign policy goal	Political agenda	Access to data or government resources
Examples	• Malware attacks on Albania's public systems attributed to Iran (2022) • Attacks on Ukrainian telecommunications system during the Russian invasion of Crimea (2014)	• Misinformation campaign suggesting a coup against Chinese President Xi Jinping (2022) • Widely reported operations of hacking groups such as Syrian Electronic Army and Anonymous	• Ransomware attack on Ireland's Health Service Executive (2021) • Data breach of India's government ID database, Aadhar (2018) • Attack on the Bangladeshi central bank, with $81 million stolen by cyber criminals (2016)

Source: S&P Global Ratings.

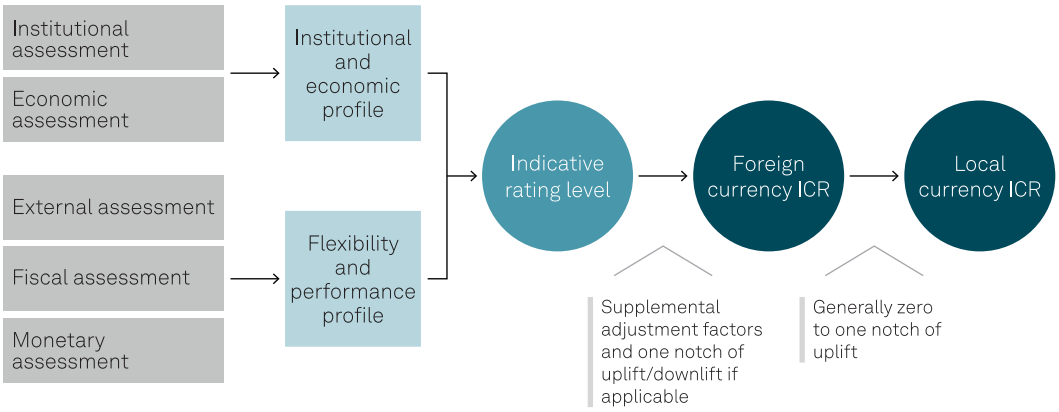
Sovereign Ratings Are Relatively Resilient To Cyber Attacks

We have not yet taken any sovereign rating actions as a direct result of cyber-related incidents.

Our sovereign criteria pertain to sovereign governments and monetary authorities and their ability and willingness to service financial obligations to commercial creditors (see "Sovereign Rating Methodology," Dec. 18, 2017). The foundation of our sovereign credit analysis rests on five pillars (see chart 1).

Chart 1

Sovereign Criteria Framework



ICR--Issuer credit rating.

Cyber incidents are unpredictable, and can affect one or more of the five credit factors. However, they are unlikely to be severe or sustained for long enough to hinder the sovereign's debt servicing ability, in our view.

Sovereigns, unlike most corporates and other entities, benefit from deep fiscal resources thanks to tax collection and other receipts from a diverse economic base. They also have non-financial resources, or advantages, such as the ability to change regulations and tax policies, the option to

draw on the wider public system (including state governments, municipalities, social security and pension systems, other government related entities, and the military), and the possibility of support from foreign governments and their agencies. We also do not consider the risk that an attack could directly hinder timely and full payment of debts to be significant as it would require third-party systems at clearing houses and banks to be affected at the same time.

For example, the cyber attacks in Costa Rica over April-May 2022 widely disrupted trade and shipping, health care and social security services, and tax collection systems. Despite temporarily causing delays and affecting the economy and revenue collection, the overall impact on Costa Rica was modest given the ability to shift to manual systems and the continued delivery of essential services.

In February 2016, cyber hackers attempted to steal nearly $1 billion (or 3% of usable reserves) from the Bangladesh Central Bank's foreign reserves account at the New York Federal Reserve, and managed to get away with $81 million. Again, despite the financial losses, this was not sufficient to weaken the sovereign external buffers or the sovereign rating.

Despite sovereigns' past resilience to cyber attacks, we are mindful of the threat of successful action and are actively monitoring for a range of incidents and potential outcomes (see table 2).

Table 2

Sovereign Cyber Attacks' Potential Impact

Institutional
Cyber attacks with a political agenda could weaken confidence in a country's institutions and, in a more extreme scenario, contribute to domestic instability or regime change. Low sovereign institutional assessments often signal relatively weak governance, which could correlate with lower cyber preparedness and defenses, and thus higher impact from cyber attacks, in our view.
Economic
A systemwide attack across several sectors over a prolonged period that affects trade, the banking system, or other critical infrastructure and services could have repercussions for businesses and households. An attack in one country could also have broader effects across geographies and sectors. For instance, the NotPetya attack in 2017 resulted in global losses exceeding $10 billion (see "Cyber Threat Brief: How Worried Should We Be About Cyber Attacks On Ukraine?," Feb. 22, 2022). Sovereign perpetrators of cyber attacks may face international sanctions that could affect broader economic activity and their access to international trade and financial markets.
External
Incidents that affect trade of goods and services could weaken current account positions and weigh on international liquidity. A potential heist linked to a central bank could also affect a country's external liquidity position.
Fiscal
Cyber operations could directly affect a sovereign's revenue collection capacity by targeting government tax systems. Spending pressure could result from increased spending on cyber security and from costs related to cyber attacks. Our sovereign criteria focuses on the fiscal position of the general government (including national, regional and local governments, and social security and pension funds). However, cyber attacks on government related enterprises or key public service entities such as utilities, hospitals, or airports could materialize as contingent liabilities for the government.
Monetary
A targeted attack on the country's central bank or wider banking system could affect monetary policy credibility and reflect weak regulatory supervision and coordination.

Source: S&P Global Ratings.

Cyber Threats Can Accompany High Geopolitical Risks, With Potentially Severe Effects For Sovereigns

Countries facing high geopolitical and external security risks could be targets of hybrid warfare (a mixture of military and cyber attacks). For this reason, where we see high geopolitical risks, we monitor whether actions on the cyber front might signal a potential escalation of a conflict (see Cyber Threat Brief: How Worried Should We Be About Cyber Attacks On Ukraine?" published Feb. 22, 2022). Such imminent or rapidly rising political/geopolitical risks can be captured as an event risk under our sovereign criteria. That differs from the potential for long-lasting and systemwide effects of a cyber incident on a sovereign's economy, finances, and institutions, which might be reflected in the respective assessments of those factors in our criteria, as outlined earlier.

The matrix below outlines how the frequency and severity of cyber attacks could affect sovereign ratings.

Chart 2

Severity/Frequency Matrix Of Cyber attacks

	Low severity	High severity
Low frequency	Unlikely to be material for sovereign ratings.	Individual cyber incidents may be material for weaker sovereigns with less diversified economies, weaker institutional settings, and less robust external and fiscal positions.
High frequency	Part of 'business as usual' management of operational risks. Cumulative impact may be material over time for less diversified economies with weaker fiscal and external buffers.	This could be akin to full blown cyber warfare or crystallization of an event risk, with potentially adverse implications for sovereign ratings.

Source: S&P Global Ratings.

How Can Governments Protect Themselves Against Growing Cyber Risks?

We believe governments will increase investment and spending on cyber security to enhance the robustness of state systems and institutions, as well as for defense and military purposes. We will continue to monitor public sector spending on cyber security to see how it translates into cyber preparedness for rated sovereigns. While advanced economies have sufficient resources to develop and deploy a comprehensive cybersecurity strategy, emerging and frontier-market sovereigns are more financially constrained, which could limit their ability to effectively plan for and respond to threats.

Key topics of discussion with sovereigns on cyber risk include:

- The country's cyber risk management strategy, policy, and framework, including key strategic priorities in this area.
- The level of cyber-risk awareness in the government and wider public sector.

- Budget and investment allocated to cyber security
- Scale of cyber events experienced and their impact on the sovereign, along with lessons learned and preventive actions taken.

Generally, we do not expect governments to eradicate cyber risk. What is critical to us is the way in which governmental institutions respond to evolving cyber threats by developing robust detection and remediation plans. For instance, cyber warfare has, to general surprise, provided just a handful of notable skirmishes in the Russia-Ukraine conflict (see "Cyber Threat Grows As Russia-Ukraine Conflict Persists," May 11, 2022). Despite high volumes of cyber attacks, the impact on Ukraine and its Western allies has so far proven more an annoyance than a serious disruption. We believe this could be partially due to increased preparedness and coordination amongst Ukraine, the EU, the U.K, and the U.S. However, this could change as the conflict continues.

We think it is likely that cyber attacks on sovereigns will become more sophisticated. The inevitably wider employment of governments' digital capabilities must therefore be accompanied by a strengthening and broadening of cyber defenses and a stronger cyber risk management culture, including the enhancement of cyber risk management frameworks.

Related Research

- Cyber Trends and Credit Risks, Oct 25, 2022.
- Cyber Risk In A New Era: International Public Finance Is A Target, July 19, 2022
- Cyber Threat Grows As Russia-Ukraine Conflict Persists, May 11, 2022
- Cyber Threat Brief: How Worried Should We Be About Cyber Attacks On Ukraine?, Feb 22, 2022
- Cyber Risk In A New Era: The Increasing Credit Relevance Of Cybersecurity, July 14, 2021

This report does not constitute a rating action.

Contact List

PRIMARY CREDIT ANALYST

Zahabia S Gupta
Dubai
(971) 4-372-7154
zahabia.gupta@spglobal.com

SECONDARY CONTACT

Roberto H Sifon-arevalo
New York
+ 1 (212) 438 7358
roberto.sifon-arevalo@spglobal.com

SECONDARY CONTACT

Dhruv Roy
Dubai
+ 971(0)56 413 3480
dhruv.roy@spglobal.com

SECONDARY CONTACT

Valerie Montmaur
Paris
+ 33144207375
valerie.montmaur@spglobal.com

SECONDARY CONTACT

Christian Esters, CFA
Frankfurt
+ 49 693 399 9262
christian.esters@spglobal.com

SECONDARY CONTACT

Martin J Whitworth
London
+44 2071766745
martin.whitworth@spglobal.com

SECONDARY CONTACT

Paul Alvarez
Washington D.C.
+1 2023832104
paul.alvarez@spglobal.com

SECONDARY CONTACT

Tiffany Tribbitt
New York
+ 1 (212) 438 8218
Tiffany.Tribbitt@spglobal.com

SECONDARY CONTACT

Nik Khakee
New York
+ 1 (212) 438 2473
nik.khakee@spglobal.com

SECONDARY CONTACT

Simon Ashworth
London
+ 44 20 7176 7243
simon.ashworth@spglobal.com

SECONDARY CONTACT

Michelle Keferstein
Frankfurt
(49) 69-33-999-104
michelle.keferstein@spglobal.com

SECONDARY CONTACT

Juili Pargaonkar
Dubai
+971-4-372-7167
juili.pargaonkar@spglobal.com