#202 - NOTE

INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

ASIA FOCUS

THE SHANGRI-LA DIALOG 2023: TOWARD THE COLD WAR 2.0 AND ITS DYNAMICS

Emmanuel Meneut / Ph.D, Lecturer at the Catholic Universities

September 2023

PRESENTATION OF THE ASIA FOCUS COLLECTION

The «Asia Focus» series offers analyses, interviews with experts or players, or notes on major works produced by specialists in the region. Its aim is to provide in-depth analysis of topical issues and offer insights into current challenges in Asia. The focus is on political, security, economic, cultural and societal dynamics.

The collection is edited by **Barthélémy Courmont**, director of research at IRIS and lecturer at the Catholic University of Lille, and **Emmanuel Lincot,** associate researcher at IRIS, professor at the Catholic Institute of Paris and sinologist. It is part of the IRIS Asia-Pacific Programme.

PROGRAMME
ASIA-PACIFIC

Due to its economic and demographic weight and the persistence of a multitude of political, strategic and security challenges, the Asia-Pacific is the focus of much attention. The IRIS Asia-Pacific Programme and its network of researchers and its network of nationally and internationally recognised researchers aim to decipher the major regional dynamics, while analysing in detail the different countries that make up the region and the challenges they face.
The fields of intervention of this programme are multiple: animation of the strategic debate; realisation of studies, reports and consultancy notes; organisation of conferences, symposiums, semnars; customised training.

This programme is directed by **Barthélémy Courmont**, director of research at IRIS and lecturer at the Catholic University of Lille.

Taking seriously the parallel of differences drawn by the great historian Niall Ferguson between the two World Wars WWI and WWII and the first Cold War CWI between the US and the USSR, and the current "Cold War CWII" between the US and China, I propose to deepen the analysis of the kind of international relations we could be confronted with in the next decade by focusing on the impact of the digital revolution. It will help us to highlight differences between the CWI's nuclear security dilemma and the CWII's cyber security dilemma like differences between the WWI's trenches warfare vs the WWII's blitzkrieg. Hence, to organize our analysis, I suggest we use a study case on energy infrastructure and companies into the context of the Shangri-La Dialog 2023, one of the most recent and important events for debating security in East and southeast Asia where cyber issues are structuring the global balance of power.

THE CASE AND THE ISSUE: "PHISHING IN THE SOUTH CHINA SEA"

Our study case[1] will be the phishing[2] cyber-attack which took place between March 2021 and June 2022 through cyber espionage on exploration companies working on the Kasawari gas field like Petronas. The origin of the cyber threat is thought to be APT 40 (= Advanced Permanent Threat). It is a group of cyber spies who penetrate the energy infrastructure and let behind them software program that could be used to disrupt the system. They are on a mission to navigate through the energy infrastructure and its control systems. The intruders haven't sought to damage the infrastructure only to prepare to do so during a crisis or a war. This cyber group is associated to the Chinese state security ministry.

Surprisingly, the Malaysian government and the targeted companies didn't react even if for the Malaysian government the Kasawari gas infrastructure are critical part of its energy security as describe in the ASEAN security outlook 2021 "the Malaysian government has introduced many initiatives to ensure energy can be supplied reliably and securely at an affordable price as investing in energy infrastructure including gas pipelines and LNG regasification terminals."

Indeed, energy infrastructure is critical because it is an enabling sector for other sectors. Without a functioning energy sector, all others of the society won't work. Hence in case of conflict, the energy sector is a strategic target since WWII either for the kinetic or cyber

[1] Sribala Subramanian, April 03, 2023, *Phishing in the South China Sea : Malaysia maintains a diplomatic silence over an alleged cyberattack on a flagship off shore energy project*. The Diplomat

[2] Phishing cyberattack is a process to trick an individual or an organizqation into disclosing confidential information by persuading the target to perform actions that unintentionally provides the attacker with access to an information system, M. Rausand S. Haugen, *Risk assessment : theory and methods,* 2020 John Wiley & sons

weapons. Each component of this sector, power line, power plant, oil or gas rig, oil or gas pipeline, oil or gas refineries or LNG is a critical infrastructure. Actually, as those components constitute a system of systems, the failure of one may unfold into a total black out through cascading effect. Information system to manage and monitor this system of systems is mainly made of administrative and an operational information systems.

Moreover, following Sribala Subramanian[3], the redline drawn by the Malaysian government, which is any physical interference with the exploitation activities, as a political threshold, was not crossed explicate the researcher Emirza adi Syailendra[4]. Generally, these exploitation activities use the operational information system.

The issue is the Malaysian diplomatic silence about the cyberattack and this cyberthreat. Does it signal an acceptable level of cybersecurity risk or a lack of mitigation ?

Our thesis is that the silence will end with the choice of a security provider for the infrastructure operational system under attack which will have the value and effects of a political alliance.

CYBERSECURITY AND FIRM PROCESSES: DIGITALIZATION, LINKAGE AND THE CYBERSECURITY DILEMMA

From the Porter model[5] of a firm value chain there is a major difference between its processes. The first type is the primary or the major processes which add value to the business activities output and rest on the operational information system. For example, in the Malaysian electricity sector national producer: Tenaga Nasional Berhad (TNB), its operational information system is made of machines (actuators on physical process), computers (SCADA) and networks used to generate, transmit and distribute power.

In the case under scrutiny a major Petronas infrastructure process is the offshore pipeline monitoring system to perform gas transportation from the gas rig productions in the Kasawari gas field to the LNG station in Bintulu off the coast of Sarawak for domestic consumption and

[3] Sribala Subramanian, April 03, 2023, *Phishing in the South China Sea : Malaysia maintains a diplomatic silence over an alleged cyberattack on a flagship off shore energy project*. The Diplomat

[4] Sribala Subramanian, April 03, 2023, *Phishing in the South China Sea : Malaysia maintains a diplomatic silence over an alleged cyberattack on a flagship off shore energy project*. The Diplomat

[5] Michael E. Porter, March–April 1979, *How Competitive Forces Shape Strategy*, Harvard business review

export to Thailand of 1.2 million tons per annum for a period of 15 years[6]. It is an operational information system.

In summary, operational information systems are programmable systems (SCADA) that interact with the physical environment. These information systems cause a direct change through the monitoring and the control of devices and actuators. The cyber-attack on an operational information system can hijack control systems that operate critical energy infrastructure with the intent to cause physical damage, as illustrated by the Stuxnet cyber-weapons used against the Iranian enrichment plant in 2009. Hence hijacking the control of an operational information system is a disruption of the primary process of the value chain. It is a political signal move since 2009.

The secondary processes are supporting the major activities and rest on the administrative information system. An administrative information system is made of the servers, the computers, the networks, and mobile devices that enable business processes in office environment. A cyber attack on an administrative information system primarily targets data availability, integrity and confidentiality. In the case under consideration the cyber-attack by APT 40 focus on the administrative information system to get commercial and strategic business plan. APT40 goals and capacities are mainly to exfiltrate proposals, minute meeting, financial data from the administrative information system[7]. So, the issue was not a purposeful crossing of the red line as taking control of the operational system of the major activities.

However, the administrative information system also contains operational data as gas depth, gas volume, chemical features;Moreover technical plans and drawings for the production infrastructure and a lot of data essential to the cyber kill chain to produce cyber-weapons to interfere with operational activities of the targeted companies.

In addition, the digitalization of the energy infrastructure sector is linking administrative information systems and operational information systems. The incentive for the firm is economic efficiency unfolding in a technical linkage between operational and administrative information system to reduce costs.

Production is scheduled to begin in 2023 so this possible articulation or linkage of the two systems is becoming a real threat in the red line…so, the red line maybe potentially already crossed. In this context the Malaysian diplomatic silence is a political fact !

[6] *Kasawari Gas Development Project, Sarawak, Malaysia* from awebsite offshore technology at url = https://www.offshore-technology.com/projects/kasawari-gas-development-project-sarawak/#catfish)

[7] Sribala Subramanian, April 03, 2023, *Phishing in the South China Sea : Malaysia maintains a diplomatic silence over an alleged cyberattack on a flagship off shore energy project*. The Diplomat

What is the feature of the security challenge ?

Energy infrastructure is a system of systems : in our Petronas' case there are the gas rig production, the gas pipeline and the LNG infrastructure, when one system is out of order, many systems will also be out of order on the full value chain. Neither the Malaysian government nor the Petronas firm can discern between spying or simply business intelligence goals of a cyber-attack and a cyber kill chain reconnaissance activity for a surprise attack on critical gas production infrastructure and gas transportation activities. This is why it kept silence. This is the interpretation problem at the heart of the security dilemma conceptualize by J. Herz[8] and R. Jervis[9]. The linkage between operational and administrative system reinforces this security dilemma.

In addition, cyber weapon confers the advantage to the attack, when a cyber warrior spent $1 building a cyber weapon through its cyber kill chain, the defender will have to spend $100 or more to protect its informational assets. Indeed, the attacker needs to identify one vulnerability and the defender must securize all the vulnerabilities of its information system. Each vulnerability requires a specific technical mitigation and some vulnerabilities are unknown to the defender : the famous zero days ! Moreover, as offense is taking advantage over defense in the cyberspace, the security dilemma unfolds into permanent intrusion activities between rivals. It was labelled cyber security dilemma[10] by B. Buchanan, it is an offensive security dilemma on the contrary of the nuclear security dilemma during the CWI, which was a defensive security dilemma. This social structure is a permanent feature of the decisional environment of the actors in the energy sector.

WHAT COULD BE THE ANSWER? CYBER RISK MANAGEMENT PROGRAM

From a functional point of view cyber security is obtained through resilience of the firm's processes. It means its ability to rapidly recover a level of activities which is acceptable for its stakeholders' survival even if it is not at the pre-cyber-attack level of quality. Resilience is obtained by redundancy of operational systems and overcapacities for the continuity plan. An operational information system will be resilient if the support processes are highly efficient, and all resources are available to quickly intervene. However, resilience could increase the

[88] Herz, J. H. (1950). *Idealist Internationalism and the Security Dilemma*. World Politics, 2(2), 157–180. https://doi.org/10.2307/2009187

[99] Jervis, R. (1978). *Cooperation Under the Security Dilemma*. World Politics, 30(2), 167–214. https://doi.org/10.2307/2009958

[10] B. Buchanan] (2017). *The Cybersecurity Dilemma: hacking, Trust and Fear Between Nations*, Oxford Academic

fixed cost of the firm if the balance between security and cost is based on the criticality of the firm's processes. Indeed, the digitalization of all the infrastructure extents the scope of the critical processes. This kind of fix cost induced by security may reach an economic deterrence level for investment of free riding. Some way to keep the cost under control is to strongly link the firm with its suppliers to reach an acceptable level of security cost. Resilience of business processes is the critical parameter to maintain trust of users and the efficiency of the country economy. Through risk management process firms and government perform the function to determine the financial cost threshold of security controls required to produce the level of trust required by the economic efficiency of the firms 'services. 80% of energy infrastructure are operated by private businesses with a cost/benefit constraint where cyber security is a permanent fixed cost.

Why security matter for both the firm and the government ?

The government and firms' stakeholders are concerned because any disruption of a product or a service safety undermined not only the firms' brand and its survivability but also the legitimacy of the government. This political lever was "discovered" by the international society in 2009 when the Stuxnet cyber-attack became public and triggered the generalization of cyber weapons for coercive diplomacy. This strategy rests on the capacity to use a weapon without explicitly using it : "coercive diplomacy is the attempt to get a target to change its objectionable behavior through either the threat to use force or the actual use of limited force[11]." By destroying 2 000 centrifuges and delaying the Iranian uranium enrichment program for 2 years under a veil of anonymity provided by the cyberspace, the US open the Pandora box of the generalization of cyber weapons for coercive diplomacy. Indeed, "coercive diplomacy is intended to be an alternative to war, even though it involves some employment of military power to achieve a state's desired objectives. […] However, coercive diplomacy represents the most dangerous way to use a state's military power; because, if coercive diplomacy fails, the state that tries it then faces two stark choices : back down or wage war. The first risks loss of face and future bargaining power; the second, loss of life and military defeat[12]." Because the use of cyber weapons may always be protected by a veil of anonymity, which is a technical feature of the cyberspace, coercive diplomacy based on the use of cyber weapons without the risk to go to war if it failed is a technique promising big results with small costs to the coercer.

More precisely, the Stuxnet cyber-attack used vulnerabilities of the Programmable Logic Controllers or PLC computer from Siemens and several "official" security certificates. Such PLC

[11] R. J. Art & P. M. Cronin*, The United States and Coercive Diplomacy*, 1/6/2003, US institute for peace
[12] R. J. Art & P. M. Cronin*, The United States and Coercive Diplomacy*, 1/6/2003, US institute for peace)

computer (or SCADA component) are essential parts of the operational information system and must be highly secured before implementation and to be used on any critical industrial infrastructure. The Iranian accused Siemens about the PLC computer lack of security and to let the US to get access to the PLC computer inside features[13]. Therefore, a supplier of a product for digital infrastructure must be politically reliable because it is a de facto security provider. It was recently illustrated by the Huawei case in the sector of the 5G communication components. Huawei has been banned by the us government because of the fear of the backdoor in its routers used for any networks included energy infrastructure networks : "We are very concerned that these companies are being financed by the Chinese government and are potentially subject to significant influence by the Chinese military, which may create an opportunity for the manipulation of switches, routers, or software embedded in American telecommunications network so that communications can be disrupted, intercepted, tampered with, or purposely misrouted[14].)"

The case of the "chip war" is an effect of this status change of the firm as a security provider not only an economic efficiency agent operating on a global market to produce goods, services, and to generate wealth. In addition, the war in Ukraine demonstrates the growing role of civil tech companies such as Microsoft, Twitter, SpaceX, etc as stakeholders in conflict zones. The main feature of this cyber security challenge is that cyber operations are continuous activities whatever the state of rivalry between great powers either exacerbated or "détente".

THE FIRM AS A SECURITY PROVIDER: LOYALTY AND TRUST

Currently, insider threat represents the major vulnerability exploited by cyber-attacks on operational information systems. An insider threat is the possibility that an employee from within the organization will use his authorized access to do harm to the security of operations and organizational assets. Hence organizations used compliance centered approach to manage cyber security risks. Organisations comply with regulations to hold themselves to specified standards and best practices. If this type of mitigation strategy is sufficient when safety is the only requirement, it is not enough when the issue is security in a coercive diplomacy environment. So, a digital company is also a security provider and this dual function

[13] Reuter, 17/4/2011, *Iran accuses Siemens over Stuxnet virus* attack

[14] quoted from Congressional Research Service https://crsreports.congress.gov R47012 : *U.S. Restrictions on Huawei Technologies: National Security*, Foreign Policy, and Economic Interests January 5, 2022

of a company as an economic and a political actor has important consequences at the international level.

The most vulnerable information system in the energy sector is the operational information system. Indeed, the main vulnerability of the energy sector is that it is a very broad ecosystem of suppliers, contractors and subcontractors which provide components and parts to the energy system of systems of critical infrastructure. These contractors' ecosystem is vulnerable to cyber-attack especially insider threat type because the securitization of employees is costly, and a lot of providers cannot increase their fixed cost to do so. They are specialized on their comparative advantage with a strong incentive from their stockholders to keep their financial results in line with the promise profits return. So, it is costly and expensive to reach an acceptable level of risk within these contractors' ecosystem.

The issue of cyber security is trusted as for any social actor facing a security dilemma. Trust from public opinion toward energy utilities services is the critical variable of the economic success of the digital revolution in the energy sector. The cyber security challenge is coming from the technology through complexity and interconnectedness. The answer to this challenge is the ability to prioritise which assets of information are most important to protect. Then based on these assets' identification, the loyalty of the employee of the associated organization becomes the security lever to produce trust within the ecosystem and the customers of the value chain.

The level of trust between energy producers and consumers is conditioned by the economic efficiency of all the firms of the energy sector to implement organizational tools to support a high level of loyalty among its work force. Finally, these actors of the energy supply chain cannot be securitized without public intervention by the government as a key partner of the organizational tools, through the legal and regulatory environment, to determine the balance between trust and cost. Intelligence and defense community are key partners of firms' ecosystem to share the burden of the trust.

Moreover, the ability to produce and to sale safety products is a necessary condition of an efficient economy and the status of a great power. This economic efficiency is the cornerstone of the power politics between Beijing and Washington on the medium term : "Superpower agreements to curb attacks can have positive effects. In 2015, US President Barack Obama and Chinese President Xi Jinping formally agreed not to knowingly conduct or support cyber operations against each other's countries. Washington and Beijing would also provide timely responses to requests for cyber security assistance and cooperate with each other to prevent and halt cybercrime. The agreement raised doubts among many onlookers who saw it as an opportunity for China to avoid sanctions imposed by Washington. However, as documented a year later, Chinese hacking attacks on US corporations and individuals decreased dramatically following the agreement[15]". It could have reduced the financial pressure of cyber security on US firms. But this agreement is under the veil of ignorance of the cyber security dilemma. As M. Doyle noticed : "Unfortunately, in subsequent years both Chinese and Russian hacks have increased[16]." Finally, the ban of Huawei and ZTE from the US market and the "chip war" confirm the difficulty to implement trust between organisms in the cyberspace due to the cybersecurity dilemma.

THE IMPACT ON THE INTERNATIONAL SOCIETY AND ORGANIZATIONS: BALANCE OF POWER AND RIVAL STANDARD REGIME

The feature of this kind of international relations is the permanent search for red lines like in the case of the Kasawari cyber-attack, in order to balance power. For example, "President Biden and President Putin reached a similar arrangement in mid-June of 2021 in Geneva. Biden declared that the United States will act against Russia if it continues with its patterns of behavior that harm the United States. Here, the harms cited are the recent JBS and Colonial Pipeline hacks conducted by Russian operatives. Biden gave Putin a list of twenty potential targets of US infrastructure that were off limits and urged the Russian president to curb ransomware hacking sites in his country. Biden also drew attention to human rights violations occurring in Russia and urged progress in nuclear arms control strategic-stability talks. Soon thereafter, Blackmatter (a revival of DarkSide, responsible for the Colonial Pipeline ransomware attack) said that it was moderating its targets and would no longer go after critical infrastructure. Other agreements could substantially assist a cyber détente[17]." By the determination of a red line on the operational system the Malaysian government includes in the defense perimeter all this kind of operational information systems which are under the cyber threat. This is a balance of power phenomena as a consequence of the cyber security dilemma and the firm as a security provider.

Moreover, the veil of ignorance of the cyber security dilemma is permanent as noticed in the ASEAN security outlook 2021 : "emerging technologies in defense and security have added a new dimension and complexity to the challenges faced in the region. The rapid advancement

[15] M. Doyle, 2022, *Cold Peace*, Liveright publishing corp, p226
[16] M. Doyle, 2022, *Cold Peace*, Liveright publishing corp, p226
[17] M. Doyle *Cold Peace*, Liveright publishing corp, p227

of technology brought about by the exponential growth of the cyberspace and various new innovations opens up new possibilities and challenges including in the defense field. These changing security environments will affect the nature of future challenges[18].”This extract describes the consequence of radical uncertainty induces by the dynamics of the digital technological breakthrough diffusion through an “S” curve (unpredictable and rapid). In the cyberspace, innovation is permanent and may be instrumentalize as a lever to shift the balance of power through coercive diplomacy or during a conflict. Indeed, one must be aware that when a conventional conflict occurred the conventional warfare technics efficiency will be amplified by the use of cyber-weapons by all parties in the conflict. It may result in protracted conflict. Moreover, as the destructive power of conventional warfare increased during the conflict, the level of connectivity decreased, hence the surface of cyber attacks is also decreasing and the utility of cyber-weapons vanished as the Ukrainian operation theater illustrate it. Nonetheless the conflict also becomes an experimental space to innovate new cyber-weapons as a game changer. For example, in coupling cyber-weapons and electronic warfare. Cyber-weapons during a conflict are especially useful as a coercive diplomacy tool toward the allied which support your enemy either to deter or to broaden the spectrum of the conflict. The issue is permanently the articulation of the private sector with security challenges underway.

In this environment, the cyber security dilemma is permanently re activated as soon as any agreement is reached. Preferences and commitment to an agreement in such strategic environment are very difficult and it requires “arms control” mechanisms to be invented. At the level of the international organizations the cyber security dilemma effect is structural.

The recent Shangri-La dialogue in June 2023 started with a session on the security implications of cyber and technological competition which illustrate the awareness of the cyber security challenge for the ASEAN member States[19]. These States are conditioned by the competition between Beijing and Washington, not only in the military sector but also economic. The competition is centered on technology which is dual with impacts on both security and wealth. Therefore, cyber security cannot be confined to economic spying issue, it is a security challenge with structural effect both on military weapons systems and critical civilian infrastructure. It also concerns territorial integrity and sovereignty. With this kind of international relations, the concept of regime is particularly relevant to describe the dynamic of the ASEAN and the great digital power, China and the US. Following Michael Drezner “the

[18] *ASEAN security outlook 2021*à l’url : https://asean.org/wp-content/uploads/2021/10/ASEAN-Security-Outlook-ASO-2021.pdf accèdé le 15/8/2023

[19] Muhamad Faizal bin Abdul Rahman, 25 mai 2023, *At SLD 2023 ASEAN defence officials must tackle technologicals issues*, the Diplomat

key variable determining whether there will be effective coordination is the size of the bargaining core among the great powers. If a large core exists, peripheral state preferences determine the process through which regulatory harmonization takes place[20]."

Concerning critical energy infrastructure, the bargaining core is constituted by the access to the energy utilities market of the ASEAN member States by the suppliers' firms from the Chinese or the US ecosystem. However, each of this ecosystem is a key component of the national cyber security of each great power. Regarding cyber security all sectors of the society are under consideration by the Chinese companies which are fully integrated to cyber security program to manage cyber threat and associated risks. The Chinese government consider China must be a global power during the transition phase from information society to digital society. Hence the development of cyber capacities which is the ability to use the cyberspace to reach political aims through levers of actions in the informational or physical environment is a key strategic goal. From a doctrinal point of view China considered cyber weapons and cyber warfare as a tool for coercive diplomacy[21]. Hence, the bargaining core is severely reduced due to the cyber security dilemma which permanently reduced the level of trust. So, "If the bargaining core between the great powers is small to nonexistent, then global regulatory coordination is far less likely, and the enforcement regime for any proposed global standard will be nonexistent. The preferences of the peripheral States, however, help to determine the tactics of great powers, IGO and NGO. If the peripheral States have moderate preferences, that is, within the zone of great power preferences, then powerful States have an incentive to attract as many allies as possible as a way to enhance the legitimacy of their own standards. This could be accomplished in a number of ways[22]."

Ironically, cyber weapons contribute to one of this way through coercive diplomacy : "another possibility is for great powers to apply their laws extraterritorially, coercing states to adopt their position[23]."In our study case, after the cyber-attack on the firms, Malaysian or foreigner, working on the Kasawari gas field "China sought blue economic partnerships with ASEAN countries" reinforcing the 2018 invitation by the Chinese offshore national company CNOOC to the regional firms[24]. The final result is not cooperation on a global or regional firms' market

[20] Drezner, D. W. (2004). *The Global Governance of the Internet: Bringing the State Back* In. Political Science Quarterly, 119(3), 477–498

[21] M. Boury, M. Collot, T. Dieudonné, B. Hubert, T. Lacharmoise, A. Sers, M Y Breh Hwing, *La cyberpuissance chinoise*, EGE, 5 juin 2022, p33

[22] Drezner, D. W. (2004). *The Global Governance of the Internet: Bringing the State Back In.* Political Science Quarterly, 119(3), 477–498

[23] Drezner, D. W. (2004). *The Global Governance of the Internet: Bringing the State Back In*. Political Science Quarterly, 119(3), 477–498

[24] Sribala Subramanian *Phishing in the South China Sea : Malaysia maintains a diplomatic silence over an alleged cyberattack on a flagship off shore energy project*. April 03, 2023, The Diplomat

firms in a stable legal environment : “regardless of the chosen strategy , the outcome is one of rival standards different fora or alliances will generate alternative sets of regulatory standards, with no clear standard accepted as international law[25].”

Moreover this security challenge is an international challenge. Indeed, critical infrastructure such as energy, are enabling infrastructure for the nominal functioning of a connected society. It requires a holistic approach because It is a system of systems with potential cascading effects and the security lever rest within a regional network of suppliers as security providers. This security provider role gives rise to a dependency risks : “which materialize when either economic or political interest diverge. Given this a holistic digital defense strategy should consider the power of stakeholders from inside and outside the government.[26]” The consequence of the development of these partnerships to increase cyber security and digital capacities especially within existing international organization like the ASEAN will fuel the regional security dilemmas and alliances.

CONCLUSION

Even if ASEAN led mechanisms are opportunities to explore confidence building which is the keystone of cyber security of civilian infrastructure, it won’t be sufficient to overcome the cyber security dilemma and the veil of technological uncertainty. Because, in last resort the trust among firms rests on the loyalty of their human resources and the status of the digital companies as security providers bound them to the national legal environment, intelligence community and interests of their government. Therefore, the consequence is a regime of rival standards for the digital and utilities firms based on the alliances system. The balance of power between Beijing and Washington is one of global security. The US through AUKUS and NATO center for cyber defense can provide Malaysian company PETRONAS with all the needed suppliers included firms from South Korea, Japan or Taiwanese companies in the energy and digital sectors. As a consequence, ASEAN member states will be part of the US alliance framework. Like the CWI and the nuclear security dilemma, the cyber security dilemma is favoring a derisking strategy of decoupling the digital and utilities suppliers’ ecosystem between the US and China.

[25] Drezner, D. W. (2004). *The Global Governance of the Internet: Bringing the State Back In*. Political Science Quarterly, 119(3), 477–498

[26] Drezner, D. W. (2004). *The Global Governance of the Internet: Bringing the State Back In*. Political Science Quarterly, 119(3), 477–498

Strategic expertise in complete independance

PROGRAMME
ASIA-PACIFIC

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

2 bis, rue Mercœur - 75011 PARIS / France
+ 33 (0) 1 53 27 60 60
contact@iris-france.org

iris-france.org

IRIS is one of the main French think tanks specialising in geopolitical and strategic issues. It is the only one to have the singularity of combining a research centre and a teaching centre delivering diplomas, via its IRIS Sup' school, a model that contributes to its national and international attractiveness.
IRIS is organised around four areas of activity: research, publication, training and event organisation.