Challenges in Measures against Digital Influence Operations: Why can't the EU/US deal with the methods used by China, Russia, and Iran?

Kazuki Ichida
(Visiting Researcher, Cyber Security Research Institute, Meiji University)
April 15, 2024

Abstract

The digital influence operation measures being undertaken in the EU and the US focus on dealing with disinformation, which in turn includes dealing with foreign interference and major social media platforms. However, the main aim of the CRI (China, Russia, and Iran) operation is to widen the polarization and distrust that already exist within their counterparts, and the use of disinformation and major social media platforms is only one of the ways to do so. The effectiveness of EU and US measures is limited in scope because the CRI can use other options to circumvent them. Since the attacker's goal is to divide the target country and spread distrust, it is essential for the defender to have an overarching understanding of the domestic situation in order to conduct research and to cope with the influence operation. However, surveys and research often involve case studies, and the overall picture is rarely examined, so effective findings are scarce. Current countermeasures, which are symptomatic treatments lacking a holistic picture, tend to fall into alarmism that issues indiscriminate warnings, and as a result, may deepen polarization and distrust. It is important to prioritize the understanding and sharing of the big picture in countermeasures against digital influence operations.

Changes in Digital Influence Operations by China, Russia, and Iran

Many of the measures taken by the European Union and the United States against digital influence operations focus on countering disinformation (including misinformation). The EU and the US have requested the major social media platforms and major ad networks to prevent interference using disinformation from abroad. The EU has introduced restrictions on major social networking platforms and ad networks, and the United States Cyber Command (USCYBERCOM) has taken active defense measures against Russia and other countries.

However, these countermeasures are easily evaded because they respond to individual attack methods rather than the aims of the attackers, the CRI (China, Russia, and Iran. See Table 1 for methods of digital influence operations). A report released on December 11, 2023 by the US National Intelligence Council shows that the situation is not compatible with the new methods of the CRI, as is corroborated by other sources.[1]

Table 1: Common TTPs (tactics, techniques, and procedures) and measures for digital influence operations

Attacking strategy	Summary	Effectiveness of countermeasures
State media and diplomats	Information originates from legitimate channels, such as state media and diplomats. Accounts of government diplomats and information posted are less likely	**Very weak**; It is often difficult to deal with diplomats and others.

[1] National Intelligence Council, "Foreign Threats to the 2022 US Elections," December 11, 2023. (https://www.odni.gov/ files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf); Kazuki Ichida, "in'bōron'to roshiano yoron'sōsao sodateta ōbēmin'shushugikokuno kakusa" (Conspiracy Theories and Russian Public Opinion Manipulation Bred Disparities in Western Democracies), Newsweek Japan, May 10, 2023. (https://www.newsweekjapan.jp/ichida/2023/05/post-46.php); Rossine Fallorina, Jose Mari Hall Lanuza, Juan Gabriel Felix Ferdinand Sanchez II, Jonathan Corpus Ong, Nicole Curato, "The Evolution of Disinformation in Three Electoral Cycles," Internews (June 29, 2023). (https://internews.org/resource/from-disinformation-to-influence-operations-the-evolution-of-disinformation-in-three-electoral- cycles/); Samuel Woolley, *Manufacturing Consensus* (New Haven: Yale University Press, 2023); Brad Smith, "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, June 22, 2022. (https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine- early-lessons-from-the-cyber-war/); Kazuki Ichida, "Maikurosofutoshano repōtowa ēkyōkōsakuni shōten'o ateteita *Defending Ukraine: Early Lessons from the Cyber War*" (Microsoft Report Focused on Influence Operations, *Defending Ukraine: Early Lessons from the Cyber War*), Kazuki Ichida's Notebook, July 2, 2022.(https://note.com/ichi_twnovel/n/n2cd93a5de9ab)

Attacking strategy	Summary	Effectiveness of countermeasures
	to be removed from social media platforms.	
Proxy	Dissemination of information from think tanks, non-profit organizations, and media outlets that ostensibly have no government involvement, but in fact do. Doppelgangers such as Russia's "Election Watch" and "Lies of Wall Street," as well as "News Front," are well known.	**Weak**; However, the reality of proxies is much better understood.
Use of AI	Generate and use images and video text utilizing LLM (Large Language Models).	**Not known**; Methodology is still under development
CIB (Coordinated Inauthentic Behavior)	Social media abuse. There are various methods such as bots, trolls, and account hacking. Spamouflage by China is well known.	**Strong**; Effective countermeasures are being established.
Hacks & leaks	Influence by hacking and publishing stolen information. The Russian "Tainted Leaks" and hacking into the Democratic Party of the US are well known instances. Sometimes the stolen information is misused.	**Strong**; Effective countermeasures are being established.
Small-scale social media	Actors use smaller, less-regulated social media rather than the more regulated platforms. They are also increasingly using encrypted instant messaging services such as Telegram.	**Very weak**; The actual situation has not been identified or a contermeasure has not been established.
Linked with major social media	In conjunction with the above strategies, small social media and messenger posts are reprinted on	**Very weak**; In addition to the difficulty of

Attacking strategy	Summary	Effectiveness of countermeasures
	major social media. Not only is this done by the concerned parties, but sympathizers in the other country may also cooperate.	ascertaining the situation, it is also difficult to deal with it when the sympathizers are one's own citizens.
Decentralization	In parallel with the above strategies, attacks are done via dozens of social media.	**Weak**; Major soial media can be addressed.
Interlocking with counterpart sympathizers	The CRI spreads narratives that are easy for individuals, groups, and media within the other country to sympathize with, and itself spreads narratives that are convenient within the other country. They are more likely to resonate with the other party's domestic anti-mainstream groups (RMVEs, conspiracy theorists, rightists, etc.).	**Very weak**; This is difficult to deal with, as countermeasures would conflict with freedom of speech and expression.
Information laundering	By having the information reprinted in the other country's media, it becomes easier to gain credibility.	**Very weak**; Not currently addressed.
Perception hacking	When an influence operation is exposed, disseminating that information in turn can foster anxiety and distrust towards all forms of information within the target country. Lately, there have been instances where "not carried out" cyber attacks or influence operations are voluntarily disclosed, aiming to exploit the effects of perception hacking.	**Very weak**; In principle, this is impossible to deal with.

Source: Kazuki Ichida, "Nisen'nijūyonen'sen'kyono toshi sekaino arikataga kawarukamo shirenai” (Election Year 2024 May Change the Way the World Works), Newsweek Japan, January 10, 2024. (https://www.newsweekjapan.jp/ichida/2024/01/2024.php)

Russia also tried to deepen polarization and distrust within the US in the 2016 US presidential election,[2] as well as in the BLM (Black Lives Matter) movement.[3] The EU and the US are aware of this, but have failed to deal with it effectively, and are still using symptomatic measures, mainly against disinformation.[4] To take advantage of domestic divisions and distrust in the target country, one can incite, cooperate with, and express support for groups and individuals within the country (Types 3 and 4 in Table 2). The main actors are the domestic groups and individuals in the other country.

Table 2: Four classifications of digital influence operations

Activity		Judgment	Whether the measure is targeted		Current measures
			Domestic	Foreign	
Type 1	Self-execution	Clear hostile interference	**Not targeted by measures against digital**	Yes	Yes
Type 2	Instructions, orders	Interference and Judgment		Yes	Yes
Type 3	Incitement, cooperation	Gray zone		Poor	No

[2] Renee DiResta, Kris Shaffer, Becky Ruppel, David Sullivan, Robert Matney, Ryan Fox, Jonathan Albright, Ben Johnson, ”The Tactics & Tropes of the Internet Research Agency,” Congress of the United States, October 2019. (https://digitalcommons.unl.edu/senatedocs/2/); Philip N. Howard, Bharath Ganesh, Dimitra Liotsiou, John Kelly, Camille François, ”The IRA, Social Media and Political Polarization in the United States 2012-2018,” University of Oxford, October 2019. (https://digitalcommons.unl.edu/senatedocs/1/)

[3] On April 17, 2015, ZeroFOX sent an email to the Mayor of Baltimore, ”Crisis Management,” that mentions Russian interference. The reference has now been deleted; Kazuki Ichida and Kayoko Ezoe, *Han’zai jizen’ sōsa shirarezaru bēkoku kēsatsutōkyokuno gijutsu* (*Crime ’Advance’ Investigation: The Unknown Techniques of U.S. Police Authorities*), Kadokawa Shinsho, 2017, chapter 1; Donie O’Sullivan, Dylan Byers, ”Exclusive: Fake Black Activist Accounts Linked to Russian Government,” CNN, September 27, 2017. (https://money.cnn.com/2017/09/28/media/blacktivist-russia-facebook-twitter/index.html)

[4] Alina Polyakova, Marlene Laruelle, Stefan Meister, Neil Barnett, “The Kremlin’s Trojan Horses,” Atlantic Council, November 15, 2016 (https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/); Alina Polyakova, Markos Kounalakis, Antonis Klapsis, Luigi Sergio Germani, Jacopo Iacoboni, Francisco de Borja Lasheras, Nicolás de Pedro, ”The Kremlin’s Trojan Horses 2.0,” Atlantic Council, November 15, 2017, (http://www.atlanticcouncil.org/publications/reports/the-kremlin-s-trojan-horses-2-0); Alina Polyakova, Flemming Splidsboel Hansen, Robert van der Noordaa, Øystein Bogen, Henrik Sundbom, ”The Kremlin’s Trojan Horses 3.0,” Atlantic Council, December 4, 2018, (https://www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlins-trojan-horses-3-0/)

Activity		Judgment	Whether the measure is targeted		Current measures
			Domestic	Foreign	
Type 4	Support statement, indirect support	Gray zone	**influence operations**	No	No

Note: Light blue cells = condemnable, but enforceable measures are difficult and likely to be repudiated.

Source: Kazuki Ichida, “Kotoshino furikaeri shūkaiokureno jōhōsen’taisakuto kōgekino shin’kokuna kairiga susumu” (Review of the Year; The Serious Divergence between Lapsed Information Warfare Measures and Attacks Continues), Kazuki Ichida’ s Notebook, December 28, 2023 (https://note.com/ichi_twnovel/n/n3b271f0fe338) modified.

On the other hand, the Type 1 and 2 methods, such as Coordinated Inauthentic Behavior (CIB), are also used, and countermeasures by the EU and the US can achieve results against these methods. Other attacks are not addressed, but only successful results are publicized, making it appear as if countermeasures are working. A prime example is the attack on the US Capitol on January 6, 2021. While there were some successes in deterring digital influence operations from China and Russia during the 2020 US presidential election, the following year saw domestic groups such as QAnon perpetrate the attack on the Capitol. A report from the Soufan Center has revealed that behind this event lay digital influence operations orchestrated by China and Russia.[5] Although this report is disputed, the QAnon-China-Russia connection is also noted in other reports listed in footnote 11, and it is believed that there was some involvement.

In recent years, there has been a setback in digital influence operations measures in the US.[6] In addition, the divisiveness and distrust in

[5] Jason Blazakis, Mohamed H. El Shawesh, Naureen Chowdhury Fink, Leela McClintock, Mollie Saltskog, Zach Schwitzky, ”Quantifying the Q Conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon,” Soufan Center, April 21, 2021. (https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by- qanon/); Zachary Cohen, ”China and Russia ’Weaponized’ QAnon Conspiracy Around Time of US Capitol Attack, Report Says,” CNN, April 19, 2021, (https://edition.cnn.com/2021/04/19/politics/qanon-russia-china-amplification/index.html); Kazuki Ichida, “Koronakade chūgokuya roshiaga hirometa kanan’no in’bōron” (QAnon Conspiracy Theory Spread by China and Russia in the COVID-19 Pandemic), Kazuki Ichida’s Notebook, October 9, 2022. (https://note.com/ichi_twnovel/n/ne1c8818d9a5c)

[6] Kazuki Ichida, “Amerikano nisejōhōtaisakuga chokumen’shiteiru mon’dai” (Problems Facing U.S. Disinformation Measures), GGR Issue Briefing, No. 32, September 1, 2023. (https://ggr.hias.hit-u.ac.jp/2023/09/01/problems-facing-us-disinformation-measures/)

the country has worsened to the point that the 2024 presidential election is expected to cause turmoil regardless of the outcome.[7]

While the CRI's interference alone has not exacerbated the polarization and distrust in the US, the three countries are playing a part. Russia has recently refrained from cyberattacks on US elections because, according to a report by the National Intelligence Council, it has determined that digital influence operations are less risky and more effective.[8]

Widespread domestic division and distrust is not only a problem in the United States, but in many other democratic countries as well, leading to the rise of populism and authoritarianism.[9] The groups promoting it are diverse, including Racially or Ethnically Motivated Violent Extremists (RMVEs) such as white supremacist groups, conspiracy theorists, and the far right, but it is highly likely that they are not different groups at all, but overlapping. Although they differ in their claims, they share a common denial of the status quo, and they change their claims depending on the time of their activities.[10] For instance, those who had been anti-vaccine advocates during the COVID-19 pandemic started simultaneously making pro-Russian and anti-Ukrainian claims when the Russian invasion of Ukraine began.[11] China and Russia have

[7] Ian Bremmer, Cliff Kupchan, "Ten Major Risks for Eurasia Group 2023," Eurasia Group, January 2024. (https://www.eurasiagroup.net/siteFiles/Media/files/Top%20Risks%202024%20JPN.pdf)

[8] National Intelligence Council, "Foreign Threats to the 2022 US Elections," December 11, 2023. (https://www.odni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf); Kazuki Ichida, "Bēkoku in'terijen'su komyunitino hyōkano hen'kakara wakaru atarashī nin'chisen'no toren'do" (New Cognitive Warfare Trends Revealed by Changes in the U.S. Intelligence Community's Assessment), Kazuki Ichida's Notebook, January 7, 2024. (https://note.com/ichi_twnovel/n/n30ab8574915c)

[9] Jon Henley, "How Europe's Far Right Is Marching Steadily into the Mainstream," The Guardian, June 30, 2023. (https://www.theguardian.com/world/2023/jun/30/far-right-on-the-march-europe-growing-taste-for-control-and-order); Pankaj Mishra, "Europe's Far Right Isn't So Fringe Anymore," Washington Post, July 19, 2023. (https://www.washingtonpost.com/business/2023/07/19/europe-s-far-right-putin-allies-are-rising-in-popularity/286def02-25ef-11ee- 9201-826e5bb78fa1_story.html); Tim Gosling, "Nationalist, Populist, Far-Right Parties Eye Rising Support across Europe," Aljazeera, September 20, 2023. (https://www.aljazeera.com/features/2023/9/20/nationalist-populist-far-right-parties-eye-rising-support-across-europe)

[10] Aoife Gallagher, Ciarán O' Connor, Francesca Visser, "Uisce Faoi Thalamh: Summary Report," Institute for Strategic Dialogue, November 20, 2022. (https://www.isdglobal.org/isd-publications/uisce-faoi-thalamh-summary-report/); Jan Rathje, "From the Crisis to the Reich Post -Pandemic Developments of 'Reichsbürger' and Sovereignists in Germany," Center for Monitoring, Analysis and Strategy, November 5, 2023. (https://cemas.io/en/publications/from-the-crisis-to-the-reich/); Kazuki Ichida, "ISDno ichiren'no hōkokushowa jōhōno ekoshisutemuno hōkatsutekichōsadatta" (ISD's Series of Reports Was a Comprehensive Survey of the Information Ecosystem), Kazuki Ichida's Notebook, November 28, 2023. (https://note.com/ichi_twnovel/n/n6c8c44b74953)

[11] Elise Thomas, "QAnon Goes to China - Via Russia," Institute for Strategic Dialogue, March 23, 2022. (https://www.isdglobal.org/digital_dispatches/qanon-goes-to-china-via-russia/);

made good use of these groups.

Existing research on the need to understand the big picture

The problem that countermeasures to digital influence operations have remained symptomatic has been pointed out in the past. Alicia Wanless has repeatedly stressed the importance of looking at the big picture.[12] According to Wanless, case studies, experiments, and surveys of high-profile cases in the media, such as elections and conflicts, are currently the norm, but they fail to capture the whole picture, not to mention the underlying causes, and Wanless claims the importance of capturing the information ecosystem. However, there are difficulties in attempting to uncover the whole picture, such as funding and the fact that it spans multiple fields of expertise. Instead, it is much easier to simplify by blaming Russia, 4chan, etc., for the results.

In the paper "Thinking Clearly about Misinformation," Li Qian Tay and colleagues focus on causal inference to summarize the issues and argue that understanding causality is necessary to consider the effects and countermeasures of digital influence operations. The authors also argue that different research studies present different hypotheses and causal models,

Kazuki Ichida, *Ukuraina shin'kōto jōhōsen'* (*Ukraine Invasion and Information Warfare*), Fusosha Shinsho, 2022; Kazuki Ichida, "Sekai kakuchide dōjihassēshita han'wakuchin'kara shinro hatsugen'eno ten'kan'" (The Simultaneous Worldwide Anti Conversion from Vaccine to Pro-Russia Statements), Kazuki Ichida's Notebook, March 31, 2022. (https://note.com/ichi_twnovel/n/nce3b3fc468a7); Mark Hay, "Pandemic and Anti-vaxxer Conspiracy Theorists are Making the Ukraine Crisis All About Them," Daily Beast, March 22, 2022. (https://www.thedailybeast.com/pandemic-and-anti-vaxxer-conspiracy-theorists-make-ukraine-crisis-all-about-them); Laura KayaliI, Mark Scott, "Anti-vax Conspiracy Groups Lean into Pro-Kremlin Propaganda in Ukraine," Politico, March 17, 2022. (https://www.politico.eu/article/antivax-conspiracy-lean-pro-kremlin-propaganda-ukraine/); Josh Butler, Sarah Martin, "Australian Online Anti-Vaccine Groups Switch to Putin Praise and Ukraine Conspiracies," The Guardian, March 1, 2022. (https://www.theguardian.com/australia-news/2022/mar/02/australias-anti-vaccine-groups-switch-focus-to-putin-praise-and-ukraine- conspiracies); Graig Graziosi, "Anti-vax Conspiracy Theorists in US Turning to Anti-semitic Pro-Putin Propaganda, Report Says," The Independent, March 2, 2022. (https://www.independent.co.uk/news/world/americas/us-politics/putin-propaganda-usa-conspiracy-theorist-b2027230.html); Sheera Frenkel, Stuart A. Thompson, "How Russia and Right-Wing Americans Converged on War in Ukraine," The New York Times, March 23, 2022. (https://www.nytimes.com/2022/03/23/technology/russia-american-far-right-ukraine.html)

[12] Alicia Wanless, "Seeing the Disinformation Forest Through the Trees: How to Begin Cleaning Up the Polluted Information Environment," The Forum Network, November 13, 2023. (https://www.oecd-forum.org/posts/seeing-the-disinformation-forest-through-the-trees-how-to-begin-cleaning-up-the-polluted- information-environment); Alicia Wanless, "There Is No Getting Ahead of Disinformation Without Moving Past It," Lawfare, May 8, 2023. (https://www.lawfaremedia.org/article/there-is-no-getting-ahead-of-disinformation-without-moving-past-it)

and reach different conclusions.[13] According to Tay et al., there are hypotheses and assumptions that dis/misinformation or conspiracy theories are caused by social backgrounds such as inequality, polarization, and the rise of populism, as well as distrust of the society; there are also hypotheses that misinformation is the cause of such backgrounds, and that such backgrounds and misinformation influence each other. Different hypotheses naturally lead to different conclusions. Tay et al. point out the oversight of factors that can occur in data analysis using randomized controlled trials with causal diagrams. This is a problem that arises as a result of prioritizing the convenience and feasibility of the research method. Therefore, Tay et al. recommend a method that is in line with the actual situation, a comprehensive approach based on causal inference, and the use of findings from cognitive science.

While causal inference is necessary to address digital influence operations, there is a tricky problem. As Judea Pearl points out, the results of causal inference follow the causal model chosen subjectively by the analyst, and different analysts using different causal models may get different results, both of which are correct.[14] Furthermore, in many cases, a less comprehensive model makes it easier to assign blame and take countermeasures. It is tempting to use a less comprehensive model that allows existing methodologies to be applied if they have been scientifically validated. Rather than choosing the best solution to the problem, we tend to define and address the problem with an approach that is optimized for the existing methodologies. A less comprehensive model leads to partially optimal measures, which can have a negative effect on the whole.

Negative effects of ineffective measures

Compounding the problem is the negative impact of the measures and the press. Those who indiscriminately disseminate disinformation threats are called alarmists, and it has been noted that the warnings issued by alarmists reduce satisfaction with democracy itself and with the press.[15] This

[13] Li Qian Tay, Stephan Lewandowsky, Mark J. Hurlstone, Tim Kurz, Ullrich K. H. Ecker, “Thinking Clearly About Misinformation,” *Commun Psychol,* 2-4, 2024. (https://doi.org/10.1038/s44271-023-00054-5)

[14] Judia Pearl, Dana McKenzie, *In’gasuiron’no kagaku naze no toini dō kotaeruka (The Book of Why: The New Science of Cause and Effect [Kindle Edition])*, Bungeishunju, 2022, p. 166.

[15] Andreas Jungherr, Adrian Rauchfleisch, “Negative Downstream Effects of Alarmist Disinformation Discourse: Evidence from the United States,” *Political Behavior* , 2024. (https://doi.org/10.1007/s11109-024-09911-3); Kazuki Ichida, “Nisejōhōeno chūikan’kiya

mechanism is similar to a technique called perception hacking, which Russia was already using in 2016. Perception hacking refers to the practice of making people skeptical and distrustful of information and media simply by learning that "digital influence operations were taking place."

The indiscriminate warnings by governments and media since 2016 may have contributed to the retreat of democracy. In Japan, for example, the Ministry of Internal Affairs and Communications is active in combating disinformation, but of course this does not include security, nor does it include Type 3 or 4 in principle. In the US election, the USCYBERCOM is taking action, but the focus is on disinformation, and furthermore, interference from within the country is beyond its scope. Both Japan and the US focus on disinformation and not much on other issues. The result is unbalanced and biased warnings, which increases the risk of alarmism. There is also a risk that issues outside the scope will be invisible, and that a trivialized partial problem will be misinterpreted as representing the whole picture.

In recent years, an increasing number of governments and companies have outsourced countermeasures against disinformation to private companies, such as reputation management firms. These companies spread the negative impact by publishing reports promoting the threat of disinformation due to sales imperatives, or by talking about the threat and the need for countermeasures in response to media interviews.

Conclusion

As we have seen above, current measures towards digital influence operations are not able to capture the entire picture, and therefore, they are only addressing problems within the scope of existing methodologies, and not selecting the best solution. Even if huge amounts of data are analyzed, each research study has a different way of looking at the problem, which is the premise for the analysis, so the findings cannot be integrated, and discussions are spinning out of control. Organizations and regulations have been established, countermeasures have been taken, fact-checking and takedowns of disinformation providers have been carried out, and it appears that results have been achieved – but in reality, there has been no improvement. In fact, these measures may even be having the opposite

hōdōga min'shushugio suitaisaseru = kēkaishugishano risuku" (Alerting and Reporting on Disinformation Declines Democracy = Alarmist Risk), Kazuki Ichida's Notebook, January 17, 2024. (https://note.com/ichi_twnovel/n/n02d7e7230e8b) effect. Meanwhile, digital influence operations by the attackers – China, Russia, Iran, and other authoritarian countries – are evolving their methods and cross-referencing effective attack techniques, resulting in increasingly similar TTPs.

In Europe, the US and Japan, the trend is likely to be toward more regulation that is unlikely to be effective. In their earlier paper, Tay et al. argued that alarmism increases consent to regulation. The focus is then skewed, which further exacerbates alarmism. In addition, the regulation of increasing amounts of disinformation often requires a systemic response, but the implementation of such a system is likely to lead towards authoritarianism. This is because all systems have ideas and intentions woven into them at the time of design and development, and operating those systems means following those ideas and intentions. The strong linkage of ideology to specification was demonstrated at the World Congress on International Telecommunications (WCIT-12).[16] The destination of alarmism is increased censorship and suppression of speech.

It is necessary to switch to a comprehensive approach at an early stage and to take measures based on an overall picture.

【Translated by】
Tomohito Nakano (Master's student, School of International and Public Policy, Hitotsubashi University)

Kazuki Ichida Profile

After managing several IT companies, Kazuki Ichida became a permanent resident of Canada in 2011 and moved to Vancouver. At the same time, he made his debut as a novelist. He has published many novels about cyber crimes that could happen in real life, as well as books and reviews about the manipulation of public opinion on the Internet. In recent years, he has written extensively on digital influence operations.

[16] Japan Network Information Center, "Domein'mēo chūshin'to shita in'tānettoporishīrepōto 2013nen 1gatsugō WCIT2012no kekkani tsuite" (Internet Policy Report with a Focus on Domain Names January 2013 - Results of WCIT 2012). (https://www.nic.ad.jp/ja/in-policy/policy- report-201301.pdf); Takehito Deguchi, "Sekai kokusaiden'kitsūshin'kaigi(WCIT-12) kekka hōkoku (sōkatsu)" (Report on the Results of the World Conference on International Telecommunications (WCIT-12)), *ITU Journal*, 43(2), 2013. (https://www.ituaj.jp/wp-content/uploads/2013/05/WCIT12.pdf)