

Finding information on the political implications of the 2018 Japanese Cybersecurity policy is a difficult task to say the least. There is available information about how the policy was initially widely debated proposals, but few scholarly articles. There is some information around how the policy intended for branches of the government to interact with and report to one another, starting from the Cybersecurity Strategy Headquarters and then branching out to the lower branches of government. This, in addition to the plan to promote inter-government cooperation, delegate tasks and responsibilities, and the plan to gradually educate all sectors of the nation came under scrutiny almost from the get-go thanks to the Cybersecurity Office's Deputy Minister, Yoshitaka Sakurada. While the policy was being debated by the Japanese Diet, Sakurada was questioned about the policy and it came out that he didn't even know how to use a computer, let alone lead an entire branch of government revolving around developing the nation's cybersecurity policies (McCurry, 2018).

Despite this initial embarrassment, this new policy was panned, debated, and eventually put into practice by the Japanese Diet out of necessity, to make sure the policy was properly developed, and those overseeing it were qualified. Before the 2018 policy, they had 2 official cybersecurity policies introduced: the first in 2006 and later in 2014, dubbed the 2014 Cybersecurity Basic Law. Before the 2006 policy was introduced, cybersecurity was generally handled on an agency-level basis which at the time seemed adequate. As time went on however, that became more and more of a liability, so much so that new policies had to eventually be introduced, like the ones in 2014 and 2018 (Bartlett, 2022). While the 2014 policy laid the foundation, the 2018 policy built upon it, and added vital changes and updates to the aging

policy, to the chagrin of the more bureaucratic, conservative members of the government seeking to limit the ruling administration's policy making power.

The 2018 policy was built upon from the foundations laid by the 2014 Basic Law, which was introduced by Hirai Takuya, a backbencher politician. It was introduced to address the rising concern of cyber related threats to the nation and introduced uniform policies to the government in regard to cybersecurity but was improved upon for the 2018 policy. One such change made to the 2018 policy proposal was it gave the Cybersecurity Strategic Headquarters permission to assign part of its functions and responsibilities to other organizations within the government, both reducing the workload on the main Cybersecurity offices, and enabling lower governmental organizations to gain experience working with cybersecurity related matters (Umeda, 2018). This was frowned upon by opposing party members and politicians since it could enable them to give more power to branches of government aligned with the ruling party's interests, a huge overhanging issue during the policy proposals.

While general policy debates were held regarding the contents of the policy and amendments to the Basic Law, one major political issue surrounding the policy was the reasoning behind its proposal in the first place. At the time, the Prime Minister Shinzo Abe and his administration were seen by some political figures as advancing the government in a more militaristic direction, and as a result, some saw the 2018 proposal as yet another aggressive policy. It gave more power to government bodies, and even enabled them to delegate responsibility to lesser branches, which would have authority over certain cybersecurity, and national security related matter. Some argued this would help promote further aggressive policies, but generally it was seen as a natural advancement and progression from past policies (Oros, 2017).

Works Cited:

Bartlett, B. (2022). *Cybersecurity in Japan*. In *The Oxford Handbook of Japanese Politics* (OXFORD HANDBOOKS SERIES, p. The Oxford Handbook of Japanese Politics, 2022). Oxford University Press.

McCurry, J. (2018, November 15). *System error: Japan cybersecurity minister admits he has never used a computer*. The Guardian. Retrieved February 26, 2023, from <https://www.theguardian.com/world/2018/nov/15/japan-cyber-security-ministernever-used-computer-yoshitaka-sakurada>

Oros, A. L. (2017). *Japan's Security Renaissance: New policies and politics for the twenty-First Century*. Columbia University Press.

Umeda, S. (2018) *Japan: Basic Act on Cybersecurity Amended*. [Web Page] Retrieved from the Library of Congress, <https://www.loc.gov/item/global-legal-monitor/2018-12-26/japan-basic-act-on-cybersecurity-amended/>.