Policy Forum 11-38: North Korea’s Digital Transformation: Implications for North Korea Policy

The NAPSNet Policy Forum provides expert analysis of contemporary peace and security issues in Northeast Asia. As always, we invite your responses to this report and hope you will take the opportunity to participate in discussion of the analysis.

Recommended Citation

Peter Hayes, Scott Bruce and Dyana Mardon, "Policy Forum 11-38: North Korea’s Digital Transformation: Implications for North Korea Policy", NAPSNet Policy Forum, November 08, 2011, https://nautilus.org/napsnet/napsnet-policy-forum/north-koreas-digital-transformation-implications-for-north-korea-policy/

North Korea’s Digital Transformation: Implications for North Korea Policy

By Peter Hayes, Scott Bruce and Dyana Mardon

November 8, 2011

Nautilus invites your contributions to this forum, including any responses to this report.

CONTENTS

I. Introduction

This essay reviews the implications of the introduction and deepening of information technology in North Korea in light of the unique social structure and state controls over information flow and individual behavior found in the DPRK. It expands upon and extrapolates from the NAPSNet Special Report "North Korea on the Cusp of Digital Transformation" by Alexander Mansourov published November 1, 2011.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

II. Report by Peter Hayes, Scott Bruce and Dyana Mardon

- North Korea's Digital Transformation: Implications for North Korea Policy

By Peter Hayes, Scott Bruce and Dyana Mardon

Introduction

This essay reviews the implications of the introduction and deepening of information technology in North Korea in light of the unique social structure and state controls over information flow and individual behavior found in the DPRK.

After first reviewing North Korea's control systems and social structure, we speculate as to some of the possible levels and leverage points at which rupture in the existing regime could occur—both decentralized, and centralized. In both instances, we suggest that cell phones, the Internet, and the DPRK Intranet will not be the basis of such challenges to state and personal power of the Kim regime. Rather, these changes would take place based on preexisting personal and kin networks of trust, which might be facilitated by changes in information technology, but not based on new networks created by the use of cell phones or Inter/Intranet.

Finally, we suggest three possible approaches to increase the impact of these IT developments in the DPRK. The first is to try to "cyber-circumvent" state controls and to stimulate dissent and uprising from below—a strategy which could risk increasing political repression in the DPRK. The second is to "cyber-engage" the DPRK in order to stimulate legitimate software industry and exports (and by implication, shut down illicit software and Internet activities). The third is to "cyber-cultivate" the DPRK by providing safe Internet zones with information materials for development purposes in the DPRK, that can be transposed to the DPRK Intranet, or accessed from inside the DPRK. The natural extension of this third strategy is the export of virtual labor from the DPRK to the ROK in information-intensive industries, and the creation of virtual family reunions on a large-scale, possibly facilitated by the International Red Cross and the ROK and DPRK Red Cross committees.

North Korean Social Surveillance and Control

The DPRK is the single most-controlling state in human history, bar none. In part, this situation arose from the thousands of years of continuous political-administrative control over the population in "Korea" (the boundaries of which have moved over time), culminating in recent centuries in an intricate system of social hierarchy and courtly politics that may be termed "orthodox" hierarchy. This system, already transformed by decades of guerilla war against Japanese colonialism and occupation, was supplemented after 1948 by the political-surveillance techniques grafted onto the traditional control system by Soviet and Chinese "best practice," thereby achieving a truly totalitarian level of individual monitoring, reporting, and control without precedent in human history. This control system is designed to sustain a social system that is based on political loyalty, with many fine gradations of social status and trust based on three broad categories, true believers (about 30%), loyal but apathetic survivors (about 30%), and potential adversaries (the rest; actual opponents are disposed of quickly). These social categories transect the basic social classes of peasant, worker, soldier and intellectual into which North Korean society is organized (now supplemented by white collar worker and most recently, by a nascent merchant class). [1]

The system is further fractionated by urban versus village and capital city versus the rest, dynamics, as well as by broad regional differences (similar to those seen in South Korea) which evolved in response to the millennia of cultural development confined to specific watersheds and ridgelines that run from the mountain backbone of the Peninsula known as "baekdudegan."

This social system is truly unique. There simply isn't another one like it. Those that looked like it superficially evaporated quickly with the demise of the Soviet Union. The cross-cutting control system rests on three primary internal security organizations which have overlapping and competing responsibilities—a characteristic that is likely not an oversight but by design. These are the State Security Department (SSD), the Ministry of People's Security (MPS, formerly the Ministry of Public Security) and the Security Command. Each of these agencies is also required to be self-funding and operate networks of factories, trading companies, and smuggling operations that often lead to international arrests, sanctions, and deportations outside the DPRK.

All these entities are controlled by Kim Jong Il. As a result, most key decisions are never made. Those that are made reflect the informational organizational problems of formulation and implementation associated with centralized rule, and the idiosyncratic characteristics arising from personalized rule. In many respects, Kim runs the DPRK as an absolute king similar to orthodox pre-modern Korean government, overlaid by the modern means of administrative and political control of every aspect of individual life, to an extent that is unique to the DPRK, exceeds the control achieved anywhere else in the world today, and probably is the tightest control over individual life of any political system in human history. Thus, the "Supreme People's Assembly" of "elected" officials is a purely rubber stamp entity that meets rarely, and then only to ink major policy pronouncements by Kim Jong Il.

One consequence of such a system, apart from its obvious opacity to outsiders, is that it is unpredictable. Perched at the top and surrounded by competing cliques, Kim controls competition for access and influence by internal security agencies that conduct intimate surveillance, and a system of systematic purges combined with continuous rotation of officials across organizations, into provincial or external postings, prison camp, and in important cases, execution.

Overall, one can characterize the DPRK has having very high political and military stability, intermediate (relative to other states in the region) social and economic stability, and very poor external stability (it has lots of enemies, more than anyone else in the region).

The Social Impact of IT on this Social Structure

Some sections of the social structure are clearly immune to the effects of IT. Those in isolated "punitive" zones where the "unreliable" are sent to live, and those in prison camps, are simply disconnected from IT, or from social networks that may be "buzzing" with IT-driven traffic about change, rumors, news, etc. One can pretty much rule out about forty percent of North Koreans being affected on this basis alone.

The 30 percent of loyal but apathetic survivors will likely appreciate the efficiency gains that IT may achieve in their lives—unless it is used to automate service industries or production processes that render them and their state wage, if it is still fulfilled by the broken distribution system, superfluous. However, these strata, fragmented by social and categorical lines, are unlikely to be involved in the IT-transformation, and for the most part, would have no access to cell phones or the DPRK intra-net, let alone the Internet.

Thus, we are left with the most urban or provincial urban elite, roughly 600,000 political, military, and economic personnel who run every aspect of North Korea. These are people who are heavily invested in the regime, and are the primary target of regime surveillance. This is also the strata of greatest concern to the regime in terms of ensuring political and social stability, both in the capital city, Pyongyang, but also in the provincial cities where the distribution system has collapsed, but the locals do not (like farmers) have access to forests to forage, or any way other than scavenging for scrap and selling on the black market, to subsist. Thus, the key problem for the regime is not just Pyongyang, but the entire network of cities, and in turn the relationship between the leadership of these cities and state enterprises therein, with the military that co-exist with them, and often draw off scarce labor or resources from them for military and state projects, as well as respond to emergencies such as floods.

Informed analysts have observed that two types of instability can emerge in this system under such enormous, unrelenting stress over the last two decades. The first is a kind of regional warlordism, led by break-away military figures who team up with the locals to start to predate on the population and resources, and then network with other breakaway units and regions. This was the fond hope of some in US Forces Korea and elsewhere in the mid-late nineties. The thesis proved utterly groundless. Not an iota of solid evidence was collected to support this theory of change. In principle, however, this dynamic could emerge in the future, and at that point, an intra-net or national cell phone system could be used as an organizing tool from "inside out" (if this organizing tool was activated or manipulated from outside, whether by certain foreign governments, or by NGOs, this external intervention could be discovered quickly and would risk the swift repression and likely execution of those involved).

The second possible dynamic is slippage in support for the regime from the second and third layers of the super-elite that surround Kim Jong Il and his key family members. Obviously, the system of control is designed to ensure that such alignments that result in an overnight coup cannot occur, but, in principle, such a coup could happen and would be unknowable in advance—just as Park Chung Hee's coup in South Korea was totally unpredicted at the time. Again, such a network is highly unlikely to rely upon cell phones, let alone the DPRK Intranet, to organize such an uprising. This kind of byzantine power shift is achieved based on personal and kin networks, in turn based on cohort and family, not in text messages. Of course, some participants in such a coup effort would use IT to communicate with distant (provincial) and external (South Korean, US, Chinese and others) players, by whatever means possible, but mostly likely by satellite phone which would be the most efficient and least able to be monitored by the control agencies, to seek external support and to allay fears of civil war that could escalate to firefights and all-out war at the DMZ. However, this modality does not rely on mass mobilization, crowd-swarming strategies, etc of the kind seen in the Middle East. The social basis for such a strategy simply does not exist in the social structure of the DPRK,

and it would be very risky to pursue strategies based on transposition of this strategy from Cairo to Pyongyang.

What Can Be Said?

In light of the above, what can one say about the influence of the cell phones, the Intranet, and the extremely limited access to the Internet from inside the DPRK?

As Alexander Mansourov writes:

> "It goes without saying that the world-wide web access is still severely restricted in North Korea. With a few exceptions, including possibly several hundred elite families, individuals are not allowed yet to have private access to the global Internet. Regardless, the general population does not feel disadvantaged or deprived at not being able to use the Internet because it has very little knowledge of it, and it has never actively used even the intranet. It is safe to say that only central party, national security units, and some Cabinet-level government organizations, as well as foreign diplomatic missions, joint ventures, and foreign individuals staying in Pyongyang can have "full but monitored" access to the Internet at their workplaces and such international hotels as Koryo, Ryanggakdo, and others." (op cit, page 23)

Mansourov adds:

> "Traditionally, the State Security Department monitored most of communications on a daily basis, eaves-dropping on most of landline telephone calls, checking every fax and incoming email. However, due to the dramatic explosion of the mobile phone use, the communications flow has recently moved beyond the SSD's ability to monitor everything.
>
> Inability to sustain total information flow control is potentially a major problem for Kim Jong Il's government because of the risk that cell phones could be used for the anti-Republic spying, [2] for hostile recruitment and blackmail of government officials, [3] for psychological warfare by hostile powers, [4] for massive influx of foreign culture, [5] to organize unregulated black market flows, to implement terrorist acts by remote control, and, finally, to organize anti-government protests and uprising. Not to miss a trick, Kim Jong Il inspected the SSD and Ministry of Public Security (MPS)-run "technical offices" (responsible for monitoring public communications) and set the revolutionary tasks "to meet the new challenges of the present day'" for their staff.
>
> In future, the SSD will probably concentrate its limited technical capabilities on close surveillance of all communications by the party, government, and military cadres, as well as foreigners, while encouraging self-censorship amongst ordinary cell phone users by promoting the general belief that the authorities may observe and tap all of the contents of communications (calls, SMS, MMS, etc.) made on mobile phones, even if they actually do not do so. Interestingly, it likely that the general population, that is, the 30 percent true believers, and many if not most of the survivors, think that this is a proper measure that the state should take in order to protect the socialist system and to maintain public order—a high value to Koreans whether they live in the North or the South. In addition, to moderate the public desire to own cell phones, the government uses various propaganda tools to caution the population that cell phones may cause brain tumor, [6] increase traffic accidents, [7] and help criminals and prisoners violate the law. [8]

> The DPRK mobile communications industry crossed the Rubicon, and the North Korean government can no longer roll it back like it did in 2004 without paying severe political price. The most the authorities can do now is probably to manage its rapid expansion in such a way that will ensure that the interests of the political regime and state security are taken care of first. As Scott Bruce from the Nautilus Institute observed, 'The implication is that communication in North Korea has transitioned from a panopticon of total control to a voluntary compliance system where the government makes an example of a select group to try and force the rest of the country to stay in line (like the Chinese do).' Indeed, this is an important change in how the government seeks to control the information flow and behavior of ordinary citizens." (op cit, pages 19-20)

Thus, North Korea's digital transformation has important implication for US, and other governments', policy toward North Korea. The flip side of the increased self-censorship is that more widespread networking of critics and supporters of the regime is possible. This networking could entail communication across normally segmented and separated hierarchical levels of the North Korean system and between the different stove-piped, bureaucratic organizations in the country. We can also imagine at some point in the future when Kim Jong Un takes over the reins of power that domestic hackers might emerge within the DPRK Intranet, posing a political problem—although again, suppressing such activity might be seen as a positive step by most of the regime's loyalist and survivor classes of population.

Conversely, it would also gain support for Kim's regime from the nascent North Korean middle class that use cell phones today. Certainly, Kim Jong Il is "entrusting" these North Koreans with more freedom of communication today than ever before. By allowing the North Korean people to use a new, albeit highly controllable, communications tool, the regime may have bolstered its legitimacy with some groups closely associated with the state.

Finally, the increased use of cell phones and the intranet can result in significant economic and productivity gains for individuals. Cell phones plus access to the intranet can result in a 5-10% increase in productivity and efficiency via coordination and time management gains, as in any other industrialized, urbanized society. The increasing use of the Intranet means that technical documents from outside of North Korea which are not deemed to be a threat to the government, can be used by universities and government organizations in North Korea to support the state's development goals. It is even possible that information technology finally is being adopted in factories and production processes where computer-based automation was previously resisted fiercely by conservative managers and political officers. [9]

As Mansourov notes, In terms of IT engagement with North Korea, several opportunities have been explored. "More recently, some North Korean academic institutions and economic organizations have sought to learn the U.S. best practices in design, development, security assurance, and integration of various complex IT systems. For instance, Kim Ch'aek University of Technology has a number of joint collaborative projects in the IT field with the Syracuse University of New York. Last March, a 12-member economic delegation from the DPRK toured Qualcomm (whose technology is widely used in the South) and the Google headquarters in Mountain View, CA, revealing considerable interest in Google's search engine technology, and held an instructional seminar with staffers from several IT companies in Silicon Valley. Obviously, the U.S.-DPRK cooperation is severely hampered by the U.S. sanctions and embargoes and is unlikely to expand any time soon." (op cit, page 27)

With that in mind there are several different paths that engagement of North Koreans on IT issues could go. These include circumvention of the system, private engagement with the North Korean IT

sector along government-sanctioned lines, and cultivation of information for endogenous inquiry by select North Koreans. We will explore each of these options below:

Cyber-Circumvention

There are several options for external IT agencies, private and public, to circumvent the North Korean system, although these options are very difficult and could result in a tightening of controls in response.

As Mansourov notes, “In the past, short-wave radio broadcasts and leaflets were used to deliver the anti-regime content directly to the DPRK population as part of the psychological warfare waged against Pyongyang, but with little practical effect. Today, thanks to the digital transformation taking root in the North, foreign civil society organizations and NGOs interested in reaching out to the North Korean people can deliver a wide range of multimedia content including movies, documentaries, electronic books and journals, animation, study programs, games, electronic dictionaries, albums, electronic maps, etc., using various voice and visual information carriers ranging from radio broadcasts, to CDs, DVDs, tapes, USBs, MP3s, flash drives, and PMPs… These efforts have the potential to affect popular tastes, attitudes, beliefs, and even values, causing some changes in the day-to-day lives of the North Korean people. But, their possible impact on political behavior remains uncertain: they have failed so far to produce any observable elite or public pressure on the political regime to change.” (op cit, page 31)

Western governments and non-governmental organizations concerned can try to reach out directly to the growing number of the North Korean IT users and broadcast desirable content by penetrating the DPRK’s firewalls. Others may try more aggressive tactics, including hacking and posting anti-DPRK materials on DPRK websites, or actually bringing them down—as reportedly occurred to past DPRK websites. These attempts are unlikely to achieve more than fleeting impressions on North Koreans, and may reinforce rather than undermine loyalty to the DPRK system as disruptive, alien forces at work in a secure virtual space provided to North Koreans by the government.

Some South Korean civil society organization and security agencies have also attempted to use Chinese cell-phones or satellite phones to allow North Koreans to access more information about the outside world. These measures could work in some areas of North Korea, particularly near the Chinese boarder where they could interface with Chinese cell towers. However, these cell phones can be identified and, when they are found, are imprisoned for using an illegal cell-phone. For example, refugee networks in China and North Korea that were exposed after the arrest of Laura Ling and Euna Lee and capture of their phone complete with contacts list faced a severe crackdown from North Korean authorities. [10]

The risk posed by these circumvention efforts is that, rather than evading a controlled system, these efforts will evoke even more monitoring and a reduction or even shut-down of “soft” information flows from NGOs that would be viewed as hostile in intent by the North Korean government. An explicit statement about NGOs promulgating circumvention tools could result in a crackdown on North Korea internet-net users and even shut down existing humanitarian and engagement channels.

Cyber-Engagement

Another option is, bearing in mind multi-layered restrictions imposed by national trade embargoes and international sanctions against Pyongyang, try to cautiously exploit the emerging opportunities in the DPRK’s IT sector.

As Mansourov writes, “Western software firms can outsource software development (corporate database management, video games, cartoons, etc.) to the DPRK firms, taking into account the past experiences of the EU (Nosotek) and ROK firms operating in China (Hanabiz.com and Samsung).

International organizations focused on IT (IANA, APNIC, ITU, etc.) and academic institutions (Syracuse University) can try to extend the international standards and share best practices with their North Korean counterparts in order to influence the DPRK’s IT developments and policy-making process.

Western IT hardware manufacturers can participate in the modernization of the DPRK’s landline and satellite telecommunications networks by providing technical assistance in upgrading the obsolete equipment and improving connectivity and the quality of voice signal and data transmission countrywide.” (op cit, page 31)

The limitation of this approach is that collaboration remains firmly under the control of North Korean authorities. Changes in the political environment can result in the sudden derailment of these collaborative ventures and business arrangements and the partnerships may be limited by United Nations and country-level sanctions. Finally, the North Korean state is generally careful to isolate these activities to limit the transformative impact on DPRK citizens.

Cyber-Cultivation

A final strategy would be to promote change in North Korea by building safe zones on the global Internet for elite North Koreans to avail themselves of different resources without fear of reprisals from the North Korean government. This would entail compiling carefully designed websites, in Korean, that provide basic learning software and study materials for language, human rights, international law, sustainability, child development, development theory, demographics, public health, sewage treatment, energy use and planning, nutrition, small business, regulations, banking, etc. Such developmental and training sites might be created and maintained in "friendly" countries such as Vietnam, Indonesia, India, and China, rather than in the "western" part of the Internet.

Possible users who might be permitted to use such safe zones would include individuals in the DPRK military, intelligence community, and party that have permission to go onto the Internet and North Korean personnel who are traveling outside of the state (either for official business as part of a workshop, conference, or training, participation in an international organization, or as managers of an overseas profit center in South-East Asia or elsewhere). Such “safe zones” might be copied wholesale onto flash drives and imported to the DPRK Intranet after careful review by DPRK authorities for cyber-attack software that might be contained in such content, and for the political nature of the content.

This strategy would not lead to rapid changes in North Korea nor undermine the DPRK regime. Those outcomes are highly unlikely given the privileged status of those with full internet access in North Korea and the punitive system of familial punishment for those caught in violation of the regime’s edicts. By creating a non-antagonistic or “safe space” for motivated North Koreans to gain access to technical knowledge from outside the DPRK, this approach would support the potential long-term transformation or “softening” of the state by building technical knowledge on much need information in North Korea that would require exchanges and opening with the outside world to make use of in the DPRK’s plans for development and economic rehabilitation. Of course, many North Koreans already engage in this “best practice” and mine the Internet in their own time and manner all over the world, feeding the information back to DPRK counterparts.

The question is whether this activity could be supported more actively and directly, in ways that

could be sanctioned by the DPRK leadership. One particularly interesting option is to create virtual labor exports from the DPRK in areas of labor-intensive information processing such as medical, insurance, banking, and other records, which would provide decent work without requiring relocation of the DPRK personnel. Obviously, such virtual work would be most competitive for records in Korean language, implying that such a virtual integration of the North Korean labor force with South Korean labor demand would require a major shift in South Korean policy. This approach is consistent with the model of “networked governance” to integrate North Korea slowly into the regional system by one of South Korea’s leading political scientists, Ha Young Sun. [11]

The natural extension of this approach would be to use information technology to support virtual family reunions for families divided between North and South Korea. This idea was explored during the Kim Dae-Jung Presidency in South Korea. The South Korean company PopcomNet reached an agreement with Baeksan Computer Company in the North to explore “virtual family reunions” between the North and South. [12] Such a social use of IT would seem to have enormously rich and powerful potential to resolve conflict at an inter-societal level, and could be administered by an independent agency based, for example, in China or Indonesia, or by the International Federation of the Red Cross working with the North and South Korean national Red Cross committees to ensure the strictly humanitarian nature of the cyber-unification.

III. References

[1] For a basic account, see US Library of Congress, Country Study, “North Korea, Classes and Social Strata,” at: http://lcweb2.loc.gov/cgi-bin/query/r?frd/cstdy:@field%28DOCID+kp0044%29; and recently, Tong Yong-sung," Study on North Korean Social Class Changes,” Samsung Economic Research Institute, in Korean, September 9, 2011.

[2] DPRK on US 'Psychological Warfare' in Iraq; Urges 'Vigilance' 'Even in Peacetime'; P'yongyang *Nodong Sinmun* in Korean 04 Jul 03 p 6; Article by Staff Reporter Kim Nam-hyok: "Let Us Heighten Vigilance Against the US Imperialists' Psychological Strategic Warfare -- The 'Shock and Awe' Operation the United States Perpetrated in Iraq"

[3] DPRK on US 'Psychological Warfare' in Iraq; Urges 'Vigilance' 'Even in Peacetime'; P'yongyang *Nodong Sinmun* in Korean 04 Jul 03 p 6; Article by Staff Reporter Kim Nam-hyok: "Let Us Heighten Vigilance Against the US Imperialists' Psychological Strategic Warfare -- The 'Shock and Awe' Operation the United States Perpetrated in Iraq"

[4] Pyongyang *Rodong Sinmun* (Electronic Edition) in Korean 14 Dec 10; Special article by reporter Ri Kyo'ng-su: "The US Imperialists' Scheming Psychological Smear Campaign That Abused Modern Science and Technology;" Description of Source: Pyongyang Rodong Sinmun (Electronic Edition) in Korean -- Daily of the Central Committee of the Workers Party of Korea; posted on the Korean Press Media (KPM) website run by the pro-Pyongyang General Association of Korean Residents in Japan; URL: http://dprkmedia.com

[5] Shanghai Northeast Asian Forum WWW-Text in Chinese 05 Dec 07; Report by Shanghai Northeast Asia Investment and Consultancy Company: "A Comparative Study of Market Analysis and Profit Models of DPRK Mobile Communications Industry" DPRK Mobile Communication Industry.pdf Description of Source: Shanghai Northeast Asian Forum WWW-Text in Chinese -- Website of the Shanghai Northeast Asia Investment & Consultancy Company, a private consulting firm that conducts research and advises strategic direction for investment in the Northeast Asian region, including the DPRK.

[6] Pyongyang Korean Central Broadcasting Station via Satellite in Korean 04 Jun 11 - 05 Jun 11

[7] Pyongyang Korean Central Television via Satellite in Korean 1100 GMT 12 Aug 09

[8] US Troubled by Smartphone, KCNA, February 11, 2011

[9] See "DPRK Information Strategy-Does It Exist?" Nautilus Institute, presented at Asia Pacific Center for Strategic Studies, October 8-10, 2002, at: http://www.nautilus.org/publications/books/dprkbb/economy/DoesitExist.html Also in hard copy in Alexandre Y. Mansourov, ed., "Bytes and Bullets: Information Technology Revolution and National Security on the Korean Peninsula," Asia-Pacific Center for Security Studies: Honolulu, HI, 2005, ISBN 0-9719416-9-6.

[10] John M. Glionna, “North Korean Defectors Network Fears Crackdown”, The Los Angeles Times, August 23, 2009

[11] Y.S. Ha, Path to an Advanced North Korea by 2032: Building a Complex Networked State, Seoul National University, East Asia Institute, Asia Security Initiative Working Paper No. 10, April 2011, pp. 11-12, at: www.eai.or.kr/data/bbs/eng_report/201104131805178.pdf

[12] “South, North Korean Firms to Arrange Virtual Reunions”, Asia Times Online, May 10, 2002.

IV. Nautilus invites your responses

The Northeast Asia Peace and Security Network invites your responses to this report. Please send responses to: bscott@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.
