Defence Research and Development Canada | Recherche et développement pour la défense Canada

Survey of Android Phones

Chris Mckenzie
2 Keys Inc.

Ryan Kennedy
Sphyrna Security Inc.

Prepared by:
2 Keys Inc.
Sphyrna Security Inc.
Ottawa, Ontario
Canada
PSPC Contract Number: W7714-156010
Technical Authority: Mazda Salmania, Defence Scientist
Contractor's date of publication: March 2018

Defence Research and Development Canada

Contract Report

DRDC-RDDC-2018-C108
May 2018

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada (DRDC) using the Schedule to the *Defence Production Act*.

Defence Research and Development Canada
Survey of Android Phones

Revised 0.3
03-31-2018

Prepared for:
Mazda Salmanian

DRDC Ottawa Research Centre
3701 Carling Avenue
Ottawa, Ontario

Prepared by:
Chris McKenzie
Ryan Kennedy

2KEYS Inc.
Sphyrna Security Inc.
Ottawa, Ontario

Proprietary Notice
The information contained in this document is proprietary to the Crown. The information disclosed herein, in whole or in part, shall not be reproduced, not shall it be used by or disclosed to others for any purpose other than explicitly defined in Contract No. DND W7714-156010/B.

Due diligence shall be exercised in ensuring that the above conditions are strictly adhered to.

Abstract

The Cyber Operations and Signals Warfare (COSW) section of Defence Research and Development Canada (DRDC) has prototyped cyber operation functions developed as applications (apps) on Android devices, which run the Lineage OS (formerly known as CyanogenMod) operating system designed to operate in a mobile Ad-Hoc network (MANET). The MANET capability on Android devices necessitates that both the WiFi chip and the Lineage OS software be supportive of Ad-Hoc mode of operation. DRDC is interested in a survey of qualified existing and emerging Android phones to better understand the hardware choices available for tactical cyber research and procure a number of units of a recommended type.

DRDC has defined a set of requirements that will be used for comparison purposes. Additional requirement refinement has been included to aide in distinguishing preferred suitable Android phones.

Résumé

La section Cyberopérations et guerre de transmissions (COGT) de Recherche et développement pour la défense Canada (RDDC) a créé un prototype de fonctions de cyberopérations sous forme d'applications destinées aux appareils Android fonctionnant avec le système d'exploitation (SE) Lineage, auparavant CyanogenMod, et conçus pour fonctionner en réseau spécial mobile (MANET, pour *Mobile Ad-Hoc Network*). Pour qu'un appareil Android prenne en charge un MANET, tant la puce sans fil que le SE Lineage doivent pouvoir fonctionner en ce mode. RDDC voudrait étudier les ordinophones Android compatibles existants ou récemment mis en marché afin de mieux comprendre les options matérielles pouvant servir à la recherche cybertactique et s'approvisionner en ordinophones du type recommandé.

RDDC a cerné un ensemble d'exigences qui serviront à comparer les candidats. D'autres critères indiqués pourront servir à dégager du lot les ordinophones Android les mieux appropriés.

Change Control Record

Date	Description of Change	Affected Pages
12/15/2017	First official draft	
12/20/2017	Second draft with complete findings and recommended next steps.	
3/31/2018	Final draft with Appendix D addition	

Table of Contents

1. Introduction

The Cyber Operations and Signals Warfare (COSW) section of Defence Research and Development Canada (DRDC) has prototyped cyber operation functions developed as applications (apps) on Android devices, which run the Lineage OS (formerly known as CyanogenMod) operating system designed to operate in a mobile Ad-Hoc network (MANET). The MANET capability on Android devices necessitates that both the WiFi chip and the Lineage OS software be supportive of Ad-Hoc mode of operation. DRDC is interested in a survey of qualified existing and emerging Android phones to better understand the hardware choices available for tactical cyber research and procure a number of units of a recommended type.

DRDC has defined a set of requirements that will be used for comparison purposes. Additional requirement refinement has been included to aid in distinguishing preferred suitable Android phones.

1.1. Intended Audience

The intended audience of this report includes project stakeholders, and people charged with procurement of Android phones for DRDC.

Readers are expected to possess background knowledge in the requirements outlined by DRDC in the TA017 statement of work. Although this report provides information on key technical points, it is the responsibility of the reader to have knowledge of the underlying technology.

1.2. Document Outline

This document consists of the following sections:

- Section 1 – Introduction: provides an overview of the report;
- Section 2 – Android Phone Options: identifies the reviewed Android phone options and the early assessment criteria used to select them;
- Section 3 – Requirements and Assessment: describes the Android phone requirements and comparison assessment; and
- Section 4 – Recommendation and Conclusion: contains options for Android phone procurement.

2. Android Phone Options

A review of available Android phones which might be applicable to DRDC purposes was conducted. The following early assessment criteria was applied to identify a short list of phones which could or be of value to DRDC.

- LineageOS support;
- Latest popular Android phone releases of note where no other suitable precursor from the manufacturer exists which meet requirements. e.g. Google Pixel and Pixel 2;
- Nexmon (https://github.com/seemoo-lab/nexmon) support for phones with the Broadcom 43xx wireless chip for monitor mode setting;
- Phones which appeared to be popular in the Android OS developer community;
- Rugged, water resistant, and large capacity battery phones; and
- Perceived presence and availability in Canada.

Through the phone options review, the following manufacturers and models were identified as safe and applicable options.

- Google Nexus 5
- Samsung S7
- Google Nexus 5x
- Google Pixel
- Google Pixel 2
- OnePlus 5
- OnePlus 5t
- Caterpillar S60
- Caterpillar S41
- LG G6

The current standard DRDC Android phone, the Nexus 5, was included for comparison purposes.

See Appendix B for a list of the key identifying features of each phone.

3. Requirements and Assessment

In an effort to highlight the most suitable Android devices which meet DRDC's needs, three assessment approaches were defined:

- **Capability requirements:** The refined DRDC requirements as outlined in the TA017 task statement of work.
- **Feature comparison:** A side-by-side comparison of key features for all candidate Android phones assessed.
- **Perceived relevance and value:** A perceived relevance and value rating to aid in "getting a feel" for similar phones which meet the survey requirements.

3.1. Capability requirements

The original DRDC requirements as outlined in the TA017 task were refined to clarify the suitability of the identified phone options. The overarching Android phone requirements defined by DRDC are as follows:

- Minimum 5" screen size
- Minimum 2300mAh battery size
- LineageOS support
- LineageOS kernel can be customized and rebuilt
- LineageOS ROM can support existing TNO apps
- Kernel can be modified to support IBSS coalescence
- Internal wifi supports monitor mode
- Internal wifi supports Ad-Hoc mode
- Can be made to create a new MANET
- Can be made to connect to an existing MANET
- External USB wifi adapter support
- Bluetooth 4.0 support for external radio tethering

Note that during assessment, the LineageOS operating system version is assumed to be version 14.1, which is equivalent to Android 7.1. The latest version of Android is 8.1.

Appendix A contains the capability requirements matrix assessment. The matrix scoring is based on a Yes/No valuation.

3.2. Feature comparison

All Android phones were reviewed for key identifying features which can be used for comparison purposes when assessing the best options. These features were then mapped to a comparison matrix with highlighting to indicate the most and least desirable features of each.

Note that comparison matrix highlighting respects that assessing some feature cannot be completely conclusive. For example, phones with System on Chip (SoC) designs, including an embedded wireless chip for which there is little evidence of supporting monitor mode, are not highlighted as undesirable.

Appendix B contains the feature comparison matrix assessment. The matrix identifies key features, such as LineageOS support, Nexmon support, screen size, ram, cost, and model availabillity.

3.3. Perceived relevance and value

The below perceived value attributes were assessed with similar phones which meet the survey capability requirements. These assessment points were assigned by the assessment team at the time of this report. For example, the reliability of the Google Nexus 5 in the year 2017 is lower than it would have been at the time of

its release, while newer phones have a higher expected reliability. This assessment might also be combined with the manufacturer reputation. For example, the OnePlus 5 phone has a comparatively lower expected reliability because they are a relatively young company.

- **Developer activity/popularity:** Devices which are popular in the XDA Android phone developer and hacking community are more likely to experience longer term LineageOS support. This criterion was based on a review of forum activity for the type and quality of activity of each phone.
- **Manufacturer support:** Phone manufacturers which appear to be releasing Android OS updates for security and device driver fixes are preferred because they are obligated to also release their Android kernel source code, making it available to LineageOS. If the manufacturer has a reputation for abandoning their phones quickly, hardware and software issues may never be solved.
- **Device age:** Older devices can experience poor LineageOS device support and lack of interest from developers who are maintaining them.
- **Failure replacement expectation:** Older or lower-end devices tend to be more difficult to replace if more need to be acquired. Manufacturers will tend to have more available stock for newer, popular, higher end devices.
- **Expected reliability:** The expected reliability of the device is determined by perceived manufacturer reputation and public failure rates for Android devices. The Blancco Technology Company "State of Mobile Device Performance and Health Q2 2017" report was used to identify failure rates for larger manufacturers.
- **Perceived cost vs value:** A rating which attempts to balance the cost of acquiring the device against the total value of its features and ability to meet DRDC requirements. For example, a new and powerful device which appears to meet all requirements fully, but has a high cost for $1,000, would receive a lower perceived value.

Appendix C contains the perceived relevance and value ratings matrix. All ratings are on a scale from 0 to 5, zero being the least perceived relevance or value, and five being the most relevance or value.

4. Recommendation and Conclusion

*The best Android phone option for DRDC as of this report is the **Samsung S7**.*

Its feature set and existing compatibility with LineageOS 14.1 and Nexmon mean that it will safely enjoy support for custom Android ROM development, external USB adapters, and internal wifi monitor mode. The device is IP68 waterproof rated, possesses a large 3000mAh battery and external micro SD card storage. Its quad-core CPU and 4GB of ram will perform very well. Availability is plentiful and from various procurement outlets, including Samsung directly, as mobile service providers continue to sell the model.

The only negative is the current cost is $700. The next cheaper model of comparable note would be the OnePlus 5t for $650 which is not as safe an option. The current Nexus 5 phone was sold for $400 when originally purchased at a time when the Canadian dollar had a higher valuation. There has never been another phone option to provide such an incredible combination of value and features.

Of the remaining phone options reviewed, there is no clear alternative. Almost all alternative phone choices in 2017 utilize the Qualcomm Snapdragon chipset which does not apparently support wireless monitor mode.

During this effort, the contract team has de-risked the migration from CyanogenMod to LineageOS by re-building LineageOS 14.1 for both the Nexus 5 and the OnePlus 5 which uses the Snapdragon 835 chipset.

The Nexus 5 phone with a custom LineageOS 14.1 build was able to create and join an existing MANET using the internal Broadcom bcm4339 wifi chip. The phone behaved similarly when loading the Nexmon driver for the bcm4339 wifi chip. If the driver is loaded via the Nexmon app, the internal wifi adapter can be put in monitor mode and connect to a MANET or Access Point. This configuration was applied manually.

The Snapdragon 835 is a popular new chipset that is found on three of the phone options being evaluated. Preliminary tests run on the OnePlus 5 showed that the wifi interface supports Ad-Hoc mode, but had troubles joining with existing networks. Monitor mode shows up in the capabilities list for the device and the device could be put into monitor mode without errors using the iw command, but no packets seem to appearing on the interface when capturing with tcpdump. Further research is required as it is possible there is just a different method required for putting the device in monitor mode.

External USB adapter support was confirmed by connecting a TP-Link wireless adapter to the Nexus 5 using a USB-OTG adapter cable and confirming through the Linux dmesg command that the adapter was recognized and the device firmware was successfully loaded.

An alternative option is to purchase a phone which meets all requirements except the internal wifi monitor mode support. If the phone can provide internal wifi MANET support, and external USB adapter support, it could be a viable choice albeit for more limited use cases.

In this regard, a secondary option would likely be any phone which is officially supported by LineageOS. LineageOS affords DRDC the ability to customize a tested and widely accepted Android operating system, reducing the potential for a limited custom solution.

*As of this report, the second best MANET only supporting phone is the **LG G6**.*

Feature wise it is a better choice than the Samsung S7, and close to the OnePlus 5. It has support for LineageOS and interestingly has built-in support for USB On-The-Go (OTG) which is required for external USB, such as

wireless adapters and hard drives. All other Android models require an OTG adapter cable to convert the USB host support to USB master. Availability for the G6 is also excellent.

All other manufacturers and models currently have issues with respect to the overall evaluation criteria:

- The Google Pixel and Pixel 2 phones do not have official LineageOS support yet. There is no reason to believe it won't be, but the current price for the Pixel 2 is higher than the Pixel and is the highest of any phone reviewed.

- The OnePlus 5 has been superseded by the OnePlus 5t and is no longer available for purchase from OnePlus directly. It can be acquired from Amazon Canada, but stock will be limited. The OnePlus 5t is not currently supported by LineageOS but there is no reason to believe it won't be.

- The latest Samsung S8, LG V30 and Motorola X4 are not currently supported by LineageOS. They are also all expensive. Although they are popular flag ship model phones, these manufacturers release many phones each year and not all of them can receive aftermarket developer support.

- Chinese manufacturers Huawei and Xiaomi are now selling low end phones along with a few higher end models in Canada, but stock is limited outside of mobile service providers, and LineageOS support appears limited to older, low end models.

- Sony and HTC phones were not included due to their small presence in the North American Android market and lack of aftermarket developer support.

- The Caterpillar phones were included due to the S60 possessing an interesting thermal camera and they are the only ruggedized phones in the North American market. Additionally, at 5000mAh, the S41 has the largest battery of any phone available. Unfortunately, there is no support for LineageOS and Caterpillar does not appear to make available their Android Linux kernel source code so it could be incorporated into a custom Android ROM build.

4.1. Post-procurement Work

During the de-risking effort to ensure that LineageOS 14.1 could be used as desired for customization and phone support, the contracting team identified follow on work which would be necessary to support any new phone device.

4.1.1. Build Custom LineageOS

Build and test a custom LineageOS 14.1 based ROM to support the requirements defined in section 3.1. This will include non-critical changes from the previous CyanogenMod based ROM to LineageOS. This includes the custom wallpaper, firmware, app installations, and any default settings that can be implemented, such as enabling adb by default, advanced restart, etc.

4.1.2. Recompile Native Binaries

All Android apps which include any C or C++ language binary files will need to be rebuilt for the new phone architecture. Since the release of the Nexus 5, all Android devices have migrated to 64-bit ARM CPUs. This means that previous binary files compiled for a 32-bit ARM CPU will need to be recompiled.

Additionally, the Position Independent Executable (PIE) compilation flag would be set when recompiling. The custom LineageOS build can continue to by-pass PIE binary checking as with previous CyanogenMod builds. See https://en.wikipedia.org/wiki/Position-independent_code for more information on PIE. Google introduced PIE as a security feature in Android 4.1 and enabled it as a mandatory compilation flag requirement in Android 5.0. Binaries not compiled as PIE compatible will not execute otherwise, unless PIE is disabled in the Android Linux kernel.

4.1.3. Replace Obsolete Tools

Any existing Android apps expected to be used with the new phone which use old and obsolete tools that are not made available with LineageOS should be converted to newer equivalents or versions. Specifically, use of the iwconfig and ifconfig command tools need to be changed to the newer iw and ip command tools, respectively.

4.1.4. Verify Monitor Mode Support

Verify that monitor mode will work with the internal wifi on any new phone. This would include ensuring that the interface can be used to establish TCP/IP connections within a MANET and capture monitor mode traffic simultaneously.

The Nexus 5 was tested with Lineage OS 14.1 and the Nexmon driver and custom firmware. Using the Nexmon-included Airodump applet to enable monitor mode appears to break the stock Android Settings app from being able to display Access Points. However, using the Nexmon command line tool, nexutil, to enable monitor mode appears to work and was verified using tcpdump to observe wireless beacon. Additionally, the Android Settings app was able to view and connect to an Access Point. When the Airodump applet was re-run the Access Point connection was destroyed. At this point the Android Settings app could be used to reconnect to the Access Point, while Airodump was still running.

More testing is necessary to understand if any changes are need to the IRN MC app.

4.1.5. SoC Support for MANET

Newer Snapdragon based chipsets, such as the Snapdragon 835, are found in many Android devices, including seven of the prospective phones being evaluated. Preliminary tests run on the OnePlus 5 showed that the wifi interface supports Ad-Hoc mode, but had troubles joining with existing networks. Monitor mode appears in the capabilities list for the device and using the iw command it can be put into monitor mode, but no packets seem to appearing on the interface when capturing with tcpdump. It is possible that there is a different method to enabling monitor mode, similar to how the Nexmon requires the nexutil command line tool to enable working monitor support on the Nexus 5. Specifications for the Snapdragon 835 and its chipset components are hard to determine, beyond the basic product page on the Qualcomm website. The WCN3990 is listed as the "companion chip" providing the 802.11 support, and it appears there are two SoCs within it, with the QCA6174 providing the 802.11 a/b/g/n/ac protocols. More information regarding these companion chips can be found here: https://wikidevi.com/wiki/Qualcomm_Atheros_QCA9008-TBD1

The QCA6174 chipset is already supported in the ath10k Linux kernel driver and recently (in the last year), changes have been made that reference WCN3990 support.

4.1.6. Verify External USB Adapter Support

Verify which external USB adapter support can be added to a LineageOS build. This would likely require kernel driver sources from the Kali Nethunter project to be imported as with the previous CyanogenMod based ROM. The following is a list of external USB wireless adapter firmware currently provided by Kali Nethunter:

ar9170-1.fw
ar9170-2.fw
bluetooth_rxtx.bin
carl9170-1.fw
hackrf_jawbreaker_usb.bin
hackrf_one_usb.bin
htc_7010.fw
htc_9271.fw
rt2561.bin
rt2561s.bin
rt2661.bin
rt2860.bin
rt2870.bin
rt3070.bin
rt3071.bin
rt3290.bin
rt73.bin
rtl8188efw.bin
rtl8192cfwU_B.bin
rtl8192cufw_B.bin
rtl8192defw.bin
rtl8192eu_nic.bin
rtl8712u.bin
rtl8723aufw_B_NoBT.bin
rtl8723bs_ap_wowlan.bin
rtl8723bs_wowlan.bin
rtl8723bu_wowlan.bin
rtl8821aefw_29.bin

rtl8188eufw.bin
rtl8192cfwU.bin
rtl8192cufw.bin
rtl8192eefw.bin
rtl8192eu_wowlan.bin
rtl8723aufw_A.bin
rtl8723befw_36.bin
rtl8723bs_bt.bin
rtl8723bu_ap_wowlan.bin
rtl8723fw_B.bin
rtl8821aefw.bin
rtl8192cfw.bin
rtl8192cufw_A.bin
rtl8192cufw_TMSC.bin
rtl8192eu_ap_wowlan.bin
rtl8192sefw.bin
rtl8723aufw_B.bin
rtl8723befw.bin
rtl8723bs_nic.bin
rtl8723bu_nic.bin
rtl8723fw.bin
rtl8821aefw_wowlan.bin
zd1211b_ub
zd1211b_uph
zd1211b_uphm
zd1211b_uphr
zd1211b_ur
zd1211_ub
zd1211_uph
zd1211_uphm
zd1211_uphr
zd1211_ur

4.2. Android 8.x Precaution

As a word of caution, the new Android 8.0 (Oreo) release is making its way into manufacturer hands and will begin to appear in the market place in new and updates for existing models.

In August 2017, the Arstechnica web site compiled an excellent list of the changes coming in Android 8.0 (https://arstechnica.com/gadgets/2017/09/android-8-0-oreo-thoroughly-reviewed/), which was used as a basis for investigating changes which could impact DRDC projects.

Specifically, Android 8.0 has included the following features which could cause issues for the lower level customization which DRDC has enjoyed through CyanogenMod in the past:

- Project Treble (https://source.android.com/devices/architecture/treble) might aide DRDC in the future with a Vendor API layer in between the Android OS and APIs, and vendor hardware. However this may result in old device drivers which worked perfectly for project purposes no longer providing legacy support for features such as Ad-Hoc wireless mode or monitor mode. Android is a consumer operating system, and Google has never officially supported Ad-Hoc wireless mode. Most likely however is that vendors will not want to reinvent their

Linux drivers, and they will probably just implement the Vendor API as a wrapper to their existing support. This will likely not effect external USB adapters.

- Android 8.0 will lock down how apps that utilize the Android Framework can behave in the background. This means that all apps with background functions will have to adapter to using the Job Scheduler API. This combined with the deprecated support for wake lock requests mean that free running background services will have to be re-engineered. A wake lock is a state which an app can request to prevent the device from going to sleep. This feature is used extensively in apps which need to be "always on", such as the IRN MC app for continuously issuing MANET broadcasts, or the IRN BFT app for sending an receiving blue-force tracking and text messaging information.

- Background services will now have limited location support. The Location Manager API used to acquire GPS location, and the GNSSMeasurements API is being limited to updating "a few times and hour". This means that apps which are not in the foreground will not receive timely GPS updates.

4.3 Additional De-Risking Effort

Based on the assumptions generated through the creation of this document that the Samsung Galaxy S7 phone model would be a viable candidate to host the new Lineage OS ROM development, the Lineage OS source code was downloaded, modified, and tested on a newly-acquired Samsung Galaxy S7. The details and conclusion of this effort have been described in Appendix D.

Appendix A – Capability Requirements Results

	Google Nexus 5	Samsung S7	Google Nexus 5x	Google Pixel	Google Pixel 2	OnePlus 5	OnePlus 5t	Caterpillar S60	Caterpillar S41	LG G6
Minium 5" screen size	Y	Y	Y	Y	Y	Y	Y	N	Y	Y
Minimum 2300mAh battery size	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
LineageOS[1] support	Y	Y	Y	N[3]	N[3]	Y	N[3]	N	N	Y
LineageOS[1] kernel can be customized and rebuilt	Y	Y	Y	N/A	N/A	Y	N/A	N/A	N/A	Y
LineageOS[1] ROM can support existing TNO apps[4]	Y	Y	Y	N/A	N/A	Y	N/A	N/A	N/A	Y
Kernel can be modified to support IBSS coalesce	Y	Y	Y[5]	N/A	N/A	Y[5]	N/A	N/A	N/A	Y[5]
Internal wifi supports monitor mode	Y[2]	Y[2]	N[5]	N/A	N/A	N[5]	N/A	N/A	N/A	N[5]
Internal wifi supports Ad-Hoc mode	Y	Y	N[5]	N/A	N/A	N[5]	N/A	N/A	N/A	N[5]
Can be made to create a new MANET	Y	Y	Y[5]	N/A	N/A	Y[5]	N/A	N/A	N/A	Y[5]
Can be made to connect to an existing MANET	Y	Y	Y[5]	N/A	N/A	Y[5]	N/A	N/A	N/A	Y[5]
External USB wifi adapter support	Y	Y	N[5]	N/A	N/A	Y[5]	N/A	N/A	N/A	Y[5]
Bluetooth 4.0 support for external radio tethering	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y

[1] LineageOS 14.1 (Android 7.1) assumed
[2] Monitor mode with radio tap headers supported on internal Broadcom wifi with Nexmon driver in LineageOS 14.1.
[3] No official support yet but there is evidence that it is coming. Newer phones, or phones which ship with Android 8.x may not be supported.
[4] Existing TNO apps such as Crytopipe and IRN MC will require additional effort to support LineageOS.
[5] Further investigation is required to conclude support.

This page left intentionally blank.

Appendix B – Feature Comparison Results

Most desirable | Preferred | Undesirable

	LineageOS support	Nexmon support	Internal wi-fi chipset	Monitor mode support (internal)	Screen size	Battery size	Water resistant	Ruggedized	Weight	Dimensions
Google Nexus 5	Y	Y	Broadcom bcm4339	Y_6	4.95"	2300mAh	N	N	130g	137.84mm x 69.17mm x 8.59 mm
Samsung S7	Y	Y	Broadcom bcm43596a0	Y_6	5.1"	3000mAh	IP68	N	152g	142.4mm x 69.6mm x 7.9mm
Google Nexus 5x	Y	N	Snapdragon 808 SoC	N	5.2"	2700mAh	N	N	136g	147.0mm x 72.6mm x 7.9mm
Google Pixel	N	N	Snapdragon 821 SoC (QCA9500)	N	5"	2770mAh	N	N	143g	143.8mm x 69.5mm x 8.5 mm
Google Pixel 2	N	N	Snapdragon 835 SoC (QCA9500)	N	5"	2700mAh	IP67	N	143g	145.7mm x 69.7mm x 7.8 m
OnePlus 5	Y	N	Snapdragon 835 SoC (QCA9500)	N	5.5"	3300mAh	IP67	N	153g	154.2mm x 74.1mm x 7.3mm
OnePlus 5t	N	N	Snapdragon 835 SoC (QCA9500)	N	6"	3300mAh	IP67	N	162g	156.1mm x 75mm x 7.3mm
Caterpillar S60	N	N	Snapdragon 617 SoC	N	4.7"	3800mAh	IP68	Y	218~g	147.9mm x 73.4mm x 12.7mm
Caterpillar S41	N	N	Mediatek MT6757 SoC	N	5"	5000mAh	IP68	Y	218g	152mm x 75mm x 12.9mm
LG G6	Y	N	Snapdragon 821 SoC	N	5.7”	3300mAh	IP68	N	163g	148.9mm x 71.9mm x 7.9mm

	CPU	CPU Architecture	Ram	Basic flash	External SD	802.11 wiFi	Mobile network	ANT+[1]	Bluetooth	USB type	Cost	Availability[3]	Release date	Discontinued
Google Nexus 5	4-core Snapdragon 800 (2.26Ghz)	ARM 32-bit	2GB	16GB	N	a/b/g/n/ac	2/3/4G LTE	N	4.0 LE	m-USB	$200-$300	Limited/ scarce	Oct-13	Y
Samsung S7	8-core M1 (2.3Ghz)	ARM 64-bit	4GB	32GB	Y	a/b/g/n/ac, MIMO	2/3/4G LTE	Y	4.2	m-USB	$700	Various/ very	Mar-16	N
Google Nexus 5x	6-core Snapdragon 808 (1.6Ghz)	ARM 64-bit	2GB	16GB	N	a/b/g/n/ac, MIMO	2/3/4G LTE	N	4.2	USB-C[2]	$400-$650	Limited/ scarce	Oct-15	Y
Google Pixel	4-core Snapdragon 821 (1.6Ghz)	ARM 64-bit	4GB	32GB	N	a/b/g/n/ac, MIMO	2/3/4G LTE	N	4.2	USB-C[2]	$900	Limited/ very	Oct-16	N
Google Pixel 2	8-core Snapdragon 835 (2.35Ghz)	ARM 64-bit	4GB	32GB	N	a/b/g/n/ac, MIMO	2/3/4G LTE	N	5	USB-C[2]	$850-$900	Various/ very	Oct-17	N
OnePlus 5	8-core Snapdragon 835 (2.45GHz)	ARM 64-bit	6GB 8GB	64GB 128GB	N	a/b/g/n/ac, MIMO	2/3/4G LTE	N	5	USB-C[2]	$730	Limited/ scarce[4]	Jun-17	N
OnePlus 5t	8-core Snapdragon 835 (2.45GHz)	ARM 64-bit	6GB 8GB	64GB 128GB	N	a/b/g/n/ac, MIMO	2/3/4G LTE	N	5	USB-C[2]	$650	Limited/ very	Nov-17	N
Caterpillar S60	8-core Snapdragon 617 (1.5Ghz)	ARM 64-bit	3GB	32GB	Y	a/b/g/n/ac, MIMO	2/3/4G LTE	N	4.1	m-USB	$700	Limited/ very	Jun-16	N
Caterpillar S41	8-core Cortex-A53 (2.3GHz)	ARM 64-bit	3GB	32GB	Y	a/b/g/n	2/3/4G LTE	N	4.1	m-USB	$600	Limited/ very	Sep-17	N
LG G6	4-core Snapdragon 821 (2.35GHz)	ARM 64-bit	4GB	32GB	Y	a/b/g/n/ac, MIMO	2/3/4G LTE	N	4.2	USB-C[5]	$650-$750	Various/ very	Feb-17	N

[1] ANT+ is a near field wireless protocol for heartrate monitors and remote control systems, similar to Bluetooth BLE but more reliable.
[2] USB-C will require new USB cables, which the phones will come with.
[3] Availability describes the procurement sources (various or limited sources) and the observed available stock (scarce or very available).
[4] The OnePlus 5 is only available from Amazon Canada. OnePlus is no longer selling it directly and instead is selling the OnePlus 5t.
[5] USB On-The-Go (UTG) supported out-of-the-box but would require a male USB-C to female USB-A adapter for TP-Link or Panda wireless adapters.
[6] Based on existence of Nexmon support or wifi chipset known to support monitor mode.

Appendix C – Perceived Relevance and Value Results

	Google Nexus 5	Samsung S7	Google Nexus 5x	Google Pixel	Google Pixel 2	OnePlus 5	OnePlus 5t	Caterpillar S60	Caterpillar S41	LG G6
Developer activity/popularity	3	5	5	5	5	4	4	0	0	5
Manufacturer support	0	4	3	5	5	4	4	0	0	4
Device age	1	4	2	4	5	5	5	2	5	5
Failure replacement expectation	1[1]	5	1[1]	3	3	2[2]	2[2]	3	5	4
Expected reliability[3]	3	4	4	5	5	4	4	5	5	4
Perceived cost vs value[4]	5	5	5	1	1	4	4	2	4	4

[1] Discontinued and Google has a poor hardware replacement support reputation.
[2] Small, newer vendor which has a reputation for releasing new, small stock models over long term support.
[3] Rating is in part based on Blancco Technology Company "State of Mobile Device Performance and Health Q2 2017" report where applicable. Available from https://www.blancco.com/resources/rs-state-of-mobile-device-performance-and-health-trend-report-q2-2017/
[4] Assessment in part based on dollar cost and ability for the phone to safely meet the needs of DRDC.

Appendix D - Samsung Galaxy S7 Custom ROM Work

An attempt to de-risk the work effort that is required to create a custom Lineage OS 14.1 build was carried out by acquiring a Samsung Galaxy S7 phone (Lineage codename: herolte) and performing the same modifications to the Lineage OS source tree that were done on the previous CyanogenMod OS build.
The procedure followed for de-risking future work revolved around the internal 802.11 driver and its support for Ad-Hoc mode and did not include support for external 802.11 USB adapters or other hardware. The following steps were used as a guide for carrying out the effort,

1. Install the TWRP Recovery image on the phone
2. Download, install and test a prebuilt Lineage OS image from their site.
3. Download, build, and test current Lineage OS source tree for the Samsung Galaxy S7.
4. Locate, download, and build (if necessary) binary executables required by the IRN MC app (iwconfig, iperf, olsrd).
5. Modify Lineage OS source code to enable Ad-Hoc mode in the Broadcom 4359 chipset driver.
6. Add the IRN MC app to the build so that it's pre-installed for testing when the ROM is installed.
7. Build and test the ROM using the IRN MC app with multiple (2 or more additional) Ad-Hoc nodes, ensuring that nodes can leave the network and rejoin after within the same scenario (BSS remains the same).

Installing TWRP

Most non-Samsung phones today are shipped with a mode of operation, called 'Fastboot', that can be used to flash file system images to the Android partition system on the phone, after a required initial step of unlocking the bootloader. Samsung phones, like the S7, come with a similar mode, called 'ODIN',, which requires a different tool on the development machine for interaction, but does not require the bootloader to be unlocked. ODIN mode on the S7 can be entered by pressing the Vol-Down, Power, and Home buttons at the same time when the phone is in the powered-off state. The tools available to communicate with the ODIN mode on the phone include the SamsungOdin provided by Samsung and an open-source tool called Heimdall, installable from the Ubuntu package repository. Because Heimdall is cross-platform and can be run on Linux, as opposed to SamsungOdin, TWRP (v3.2.1-1) was installed using the Heimdall Frontend (v1.4.0) GUI.

Testing the Prebuilt Lineage OS

A prebuilt Lineage OS build for herolte was downloaded and installed using the TWRP recovery mode, which can be entered by pressing the Vol-Up, Power, and Home buttons at the same time when the phone is in the powered-off state. The image used was from a nightly build with the name, *lineage-14.1-20180301-nightly-herolte-signed.zip.* The installed OS passed the basic testing of functionality that we would expect to work without our modifications, such as connecting the 802.11 interface to an Access Point and ensuring Root access can be enabled through the developer settings.

The Lineage OS Build

A fresh Lineage source code repository was downloaded, built, and tested on the phone as a sanity check to ensure the code base to be modified is stable. The code was built successfully without requiring source code or build file modifications, following the guide on the Lineage OS site,

https://wiki.lineageos.org/devices/herolte/build

Modifications were then made to the Lineage source code to enable IBSS coelesence in the bcmdhd driver and provide Ad-Hoc mode support by the internal Broadcom 802.11 chipset. Specifically, the file found at,

android/lineage/kernel/samsung/universal8890/drivers/net/wireless/bcmdhd4359/wl_cfg80211.c

Was edited to replace the following lines,
(wl_cfg80211.c, lines 356-362)

```
#ifndef IBSS_COALESCE_ALLOWED
#define IBSS_COALESCE_ALLOWED 0
#endif

#ifndef IBSS_INITIAL_SCAN_ALLOWED
#define IBSS_INITIAL_SCAN_ALLOWED 0
#endif
```

with,

```
#ifndef IBSS_COALESCE_ALLOWED
#define IBSS_COALESCE_ALLOWED 1
#endif

#ifndef IBSS_INITIAL_SCAN_ALLOWED
#define IBSS_INITIAL_SCAN_ALLOWED 1
#endif
```

Acquiring New Binary Executables

Because the CPU architecture on the S7 phone is different than that of the Nexus 5, new binary executable files are required in order for IRN MC to function properly. The list of the required binaries, and how they were acquired for the S7, are shown below.
Initially, the Position Independent Executable (PIE) flag requirement was going to be disabled in the Lineage OS source code by simply commenting out a line of code that checks for the flag, as was done with the previous Cybermod build, however, the newer, more exhaustive code that enforces the flag comes with more risk of misinterpretation of the expected results. Therefore, the decision was made to not disable the PIE-flag enforcement in the source code and just ensure that all binaries have been compiled with the PIE flag.

- iwconfig - Part of the Linux Wireless Tools (includes iwspy, iwlist, etc.), was built using ndk-build and the source (already including Android.mk file) from, https://github.com/LineageOS/android_external_wireless-tools
- iperf - Downloaded from the github site, https://github.com/pip1998/ndkiperf.git, and built using ndk-build.
- olsrd - Could not be built for Android from their github source tree (not olsrd nor OONF). An additional effort was carried to create a new build environment that relied on ndk-build, using the source code from the olsrd github repository.

Adding the IRN MC App

The IRN MC App (v0.2.7) was added to the Lineage OS build by adding the installable IRNMC.apk file to a newly created directory, android/lineage/packages/apps/IRNMC/,
along with a newly created Android.mk file in the same directory, with the contents,

```
LOCAL_PATH := $(call my-dir)
include $(CLEAR_VARS)
LOCAL_MODULE_TAGS := optional
LOCAL_MODULE := IRNMC
LOCAL_CERTIFICATE := media
LOCAL_SRC_FILES := IRNMC.apk
LOCAL_MODULE_CLASS := APPS
LOCAL_MODULE_SUFFIX := $(COMMON_ANDROID_PACKAGE_SUFFIX)
include $(BUILD_PREBUILT)
```

and editing the file, android/lineage/device/samsung/herolte/device_herolte.mk, to contain the lines,

```
PRODUCT_PACKAGES += \
IRNMC
```

Conclusion: Testing the Custom ROM

The custom ROM built with the above modifications was installed on the S7 phone using the TWRP recovery mode. With the phone turned on and booted into the newly installed OS, the IRN MC app was opened and configured to establish an Ad-Hoc network using the internal 802.11 interface. When the app was run to setup the network interface, the process timed out. The setup script was then run manually from the terminal and displayed errors related to the commands being sent to the 802.11 interface to setup the Ad-Hoc network.

In an attempt to troubleshoot further, a new ROM was built with a modified kernel configuration that enabled the creation of the /proc/config.gz file on the resulting system (contains the kernel configuration file used to build the kernel). However, when the resulting ROM build yielded a system that didn't seem to create the /proc/config.gz file, and with further investigating through rebuilds using different configuration files, it became apparent that it's not reliable to modify the kernel configuration file within the Lineage OS source tree.

Online searches for steps on how to build the kernel support this finding with the fact that they all seem to provide steps that involve downloading and building a kernel-only package and flashing it to the phone separately. The kernel for the S7 was downloaded from the LineageOS github site,

https://github.com/LineageOS/android_kernel_samsung_universal8890.git

and was modified to match the changes added above and with a modified kernel configuration that enabled the creation of the /proc/config.gz file on the resulting system. Unfortunately, after the newly built kernel image was flashed to the phone, the phone failed to boot up past the "Samsung Galaxy S7" init screen and displayed an error in red text at the top that reads, "Kernel is not SEANDROID Enforcing".

Because of the issues and lack of time that remained to complete the effort of de-risking the future work of a customly-build Lineage OS ROM (Cybermod 2.0), further attempts to complete the ROM build were then halted. However, the effort that was carried out succeeded in revealing that the Lineage OS source code can be modified with our required changes, rebuilt, and loaded onto a Samsung Galaxy S7 phone. In addition to the prebuilt binaries executables being made available for a future ROM build, the challenges of running the IRN MC Android app to meet requirements were narrowed down to the enabling of Ad-Hoc mode with the 802.11 interface. This issue will have to be sorted out before the Samsung Galaxy S7 can be verified as a viable candidate to run the new Cybermod 2.0 ROM with the IRN MC app.

The Phone Model(s)

Two phones with different model numbers were used; SM-G930W8 and SM-G930FD. The main difference between the models is that the SM-G930FD is manufactured with an additional SIM card slot and global cellular capabilities, whereas the SM-G930W8 has been manufactured to operate on LTE bands that are predominant in North America. The effort described above was arbitrarily done on the SM-G930FD model.

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

2 Keys Inc.
Sphyrna Security Inc.
Ottawa, Ontario
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Survey of Android Phones

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Mckenzie, C.; Kennedy, R.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
March 2018	24	0

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC - Ottawa Research Centre
Defence Research and Development Canada
3701 Carling Avenue
Ottawa, Ontario K1A 0Z4
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
05ab	W7714-156010

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2018-C108	

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Android; phone; mobile; adhoc

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

Abstract

The Cyber Operations and Signals Warfare (COSW) section of Defence Research and Development Canada (DRDC) has prototyped cyber operation functions developed as applications (apps) on Android devices, which run the Lineage OS (formerly known as CyanogenMod) operating system designed to operate in a mobile Ad-Hoc network (MANET). The MANET capability on Android devices necessitates that both the WiFi chip and the Lineage OS software be supportive of Ad-Hoc mode of operation. DRDC is interested in a survey of qualified existing and emerging Android phones to better understand the hardware choices available for tactical cyber research and procure a number of units of a recommended type.

DRDC has defined a set of requirements that will be used for comparison purposes. Additional requirement refinement has been included to aide in distinguishing preferred suitable Android phones.

Résumé

La section Cyberopérations et guerre de transmissions (COGT) de Recherche et développement pour la défense Canada (RDDC) a créé un prototype de fonctions de cyberopérations sous forme d'applications destinées aux appareils Android fonctionnant avec le système d'exploitation (SE) Lineage, auparavant CyanogenMod, et conçus pour fonctionner en réseau spécial mobile (MANET, pour *Mobile Ad-Hoc Network*). Pour qu'un appareil Android prenne en charge un MANET, tant la puce sans fil que le SE Lineage doivent pouvoir fonctionner en ce mode. RDDC voudrait étudier les ordinophones Android compatibles existants ou récemment mis en marché afin de mieux comprendre les options matérielles pouvant servir à la recherche cybertactique et s'approvisionner en ordinophones du type recommandé.

RDDC a cerné un ensemble d'exigences qui serviront à comparer les candidats. D'autres critères indiqués pourront servir à dégager du lot les ordinophones Android les mieux appropriés.