

PLEASE REFRESH, YOU SHOULD HAVE THE EDITING RIGHTS RIGHT NOW. IF IT STILL DOESN'T WORK, MAIL ME AT [d33tah@gmail.com](mailto:d33tah@gmail.com)

(I rewrote all the codenames in order and copied Schneier's descriptions where appropriate. Feel invited to add some!)

((This is Bruce: Please add the status as well, so we know what is operational and what is in development.))

(Several file formats are available which are suitable for copy-pasting from. In particular, the Word/Writer versions (.doc, .docx, and .odt) have "uncertain characters" from the OCR highlighted: <http://dccjr.com/344d3f498ee47a30ccba33a4b0d291d7/> )

## Engineering

Tool/System	Description	Status	Contacts
Cerberus Statistics Collection	Collects on-going usage information about how many users utilise JTRIG's UIA capability, what sites are the most frequently visited etc. This is in order to provide JTRIG infrastructure and ITServices management information statistics.	OPERATIONAL	JTRIG Software dDevelopers
JTRIG RADIANT SPLENDOUR	is a 'Data Diode' connecting the CERBERUS network with GCNET	OPERATIONAL	JTRIG Software Developers
ALLIUM ARCH	JTRIG UIA via the Tor network.	OPERATIONAL	JTRIG Infrastructure Team
ASTRAL PROJECTION	Remote GSM secure covert internet proxy using TOR hidden	OPERATIONAL	JTRIG Infrastructure Team

	services.		
TWILIGHT ARROW	Remote GSM secure covert internet proxy using VPN services.	OPERATIONAL	JTRIG Infrastructure Team
SPICE ISLAND	JTRIG's new Infrastructure. FOREST WARRIOR, FRUIT BOWL, JAZZ FUSION and other JTRIG systems will form part of the SPICE ISLAND infrastructure	DEV	JTRIG Infrastructure Team
POISON ARROW	Safe Malware download capability.	DESIGN	JTRIG Infrastructure Team
FRUIT BOWL	CERBERUS UIA Replacement and new tools infrastructure - Primary Domain for Generic User/Tools Access and TOR split into 3 sub-systems.	DESIGN	JTRIG Infrastructure Team
NUT ALLERGY	JTRIG Tor web browser - Sandbox IE replacement and FRUIT BOWL sub-system	PILOT	JTRIG Infrastructure Team
BERRY TWISTER	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team
BERRY TWISTER+	A sub-system of FRUIT BOWL	PILOT	JTRIG Infrastructure Team
BRANDY SNAP	JTRIG UIA contingency at Scarborough.	IMPLEMENTATION	JTRIG Infrastructure Team
WIND FARM	R&D offsite facility.	DESIGN	JTRIG Infrastructure Team
CERBERUS	JTRIG's legacy UIA desktop, soon to be replaced with	OPERATIONAL	JTRIG Infrastructure Team

	FOREST WARRIOR.		
BOMBAYROLL	JTRIG's legacy UIA standalone capability.	OPERATIONAL	JTRIG Infrastructure Team
JAZZ FUSION	BOMBAY ROLL Replacement which will also incorporate new collectors - Primary Domain for Dedicated Connections split into 3 sub-systems.	IMPLEMENTATION	JTRIG Infrastructure Team
COUNTRY FILE	A sub-system of JAZZ FUSION	OPERATIONAL	JTRIG Infrastructure Team
TECHNO VIKING	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
JAZZ FUSION+	A sub-system of JAZZ FUSION	DESIGN	JTRIG Infrastructure Team
BUMBLEBEE DANCE	JTRIG Operational VM/TOR architecture	OPERATIONAL	JTRIG Infrastructure Team
AIR BAG	JTRIG Laptop capability for field operations.	OPERATIONAL	JTRIG Infrastructure Team
EXPOW	GCHQ's UIA capability provided by JTRIG.	OPERATIONAL	JTRIG Infrastructure Team
AXLE GREASE	The covert banking link for CPG	OPERATIONAL	JTRIG Infrastructure Team
POD RACE	JTRIG'S MS update farm	DESIGN	JTRIG Infrastructure Team
WATCHTOWER	GCNET -> CERBERUS Export Gateway Interface System	OPERATIONAL	JTRIG Software Developers
REAPER	CERBERUS -> GCNET Import Gateway Interface System	OPERATIONAL	JTRIG Software Developers

DIALd	External Internet Redial and Monitor Daemon	OPERATIONAL	JTRIG Software Developers
FOREST WARRIOR	Desktop replacement for CERBERUS	DESIGN	JTRIG Infrastructure Team
DOG HANDLER	JTRIG's development network	DESIGN	JTRIG Infrastructure Team
DIRTY DEVIL	JTRIG'S research network	DESIGN	JTRIG Infrastructure Team

## COLLECTION

<b>Tool</b>	<b>Description</b>	<b>Status</b>	<b>Contacts</b>
AIRWOLF	YouTube profile, comment and video collection.	Beta release.	
ANCESTRY	Tool for discovering the creation date of yahoo selectors.	Fully Operational.	JTRIG Software Developers
BEARTRAP	Bulk retrieval of public BEBO profiles from member or group ID.	Fully Operational.	
BIRDSONG	Automated posting of Twitter updates.	Decommissioned. Replaced by SYLVESTER.	
BIRDSTRIKE	Twitter monitoring and profile collection. Click here for the User Guide.	Fully Operational.	
BUGSY	Google+ collection (circles, profiles etc.)	In early development.	
DANCING BEAR	obtains the locations of WiFi access points.	Fully Operational.	

DEVIL'S HANDSHAKE	ECI Data Technique.	Fully Operational.	
DRAGON'S SNOUT	Paltalk group chat collection.	Beta release.	
EXCALIBUR	acquires a Paltalk UID and/or email address from a Screen Name.	Fully Operational (against current Paltalk version)	
FATYAK	Public data collection from LinkedIn.	In Development.	
FUSEWIRE	Provides 24/7 monitoring of Vbulliten forums for target postings/online activity. Also allows staggered postings to be made.		
GLASSBACK	Technique of getting a targets IP address by pretending to be a spammer and ringing them. Target does not need to answer.	Fully Operational.	
GODFATHER	Public data collection from Facebook.	Fully Operational.	
GOODFELLA	Generic framework for public data collection from Online Social Networks.	In Development (Supports RenRen and Xing).	
HACIENDA	is a port scanning tool designed to scan an entire country or city. It uses GEOFUSION to identify IP locations. Banners and content are pulled back on certain ports. Content is put into the EARTHLING database, and all other scanned data is sent to GNE and	Fully Operational.	

	is available through GLOBAL SURGE and Fleximart.		
ICE	is an advanced IP harvesting technique.		
INSPECTOR	Tool for monitoring domain information and site availability	Fully Operational.	
LANDING PARTY	Tool for auditing dissemination of VIKING PILLAGE data.	Fully Operational.	
MINIATURE HERO	Active skype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists.	Fully operational, but note usage restrictions.	
MOUTH	Tool for collection for downloading a user's files from Archive.org.	Fully Operational.	
MUSTANG	provides covert access to the locations of GSM cell towers.	Fully Operational.	
PHOTON TORPEDO	A technique to actively grab the IP address of MSN messenger user.	Operational, but usage restrictions.	
RESEVOIR	Facebook application allowing collection of various information.	Fully operational, but note operational restrictions.	
SEBACIUM	An ICTR developed system to identify P2P file sharing activity of intelligence value. Logs are accessible via DIRTY RAT.		

SILVER SPECTER	Allows batch Nmap scanning over Tor.	In Development.	
SODAWATER	A tool for regularly downloading gmail messages and forwarding them onto CERBERUS mailboxes	Fully Operational.	
SPRING BISHOP	Find private photographs of targets on Facebook.		
SYLVESTER	Framework for automated interaction / alias management on online social networks.	In Development.	
TANNER	A technical programme allowing operators to log on to a JTRIG website to grab IP addresses of Internet Cafe's.	Replaced by HAVOK.	
TRACER FIRE	An Office Document that grabs the targets Machine info, files, logs, etc and posts it back to GCHQ.	In Development.	
VIEWER	A programme that (hopefully) provides advance tip off of the kidnappers IP address for HMG personnel.	Operational, but awaiting field trial.	
VIKING PILLAGE	Distributed network for the automatic collection of encrypted/ compressed data from remotely hosted JTRIG projects.	Operational.	
TOP HAT	A version of the MUSTANG and	In Development.	

	DANCING BEAR techniques that allows us to pull back Cell Tower and WiFi locations targeted against particular areas.		
--	--	--	--

## EFFECTS CAPABILITY

Tool	Description	Status	Contacts
ANGRY PIRATE	is a tool that will permanently disable a target's account on their computer.	Ready to fire (but see target restrictions).	
ARSON SAM	is a tool to test the effect of certain types of PDU SMS messages on phones / network. It also includes PDU SMS Dumb Fuzz testing	Ready to fire (Not against live targets, this is a R&D Tool).	
BUMPERCAR+	is an automated system developed by JTRIG CITD to support JTRIG BUMPERCAR operations. BUMPERCAR operations are used to disrupt and deny Internet-based terror videos or other materials. The techniques employs the services provided by upload providers to report offensive materials.	Ready to fire.	
BOMB BAY	is the capacity to increase website hits/ rankings.	In Development.	

BADGER	mass delivery of email messaging to support an Information Operations campaign	Ready to fire.	
BURLESQUE	is the capacity to send spoofed SMS messages.	Ready to fire.	
CANONBALL	is the capability to send repeated text messages to a single target.	Ready to fire.	
CLEAN SWEEP	Masquerade Facebook Wall Posts for individuals or entire countries.	Ready to fire (SIGINT sources required)	
CLUMSY BEEKEEPER	Some work in progress to investigate IRC effects.	NOT READY TO FIRE.	
CHINESE FIRECRACKER	Overt brute login attempts against online forums	Ready to fire.	
CONCRETE DONKEY	is the capability to scatter an audio message to a large number of telephones, or repeatedly bomb a target number with the same message.	In development.	
DEER STALKER	Ability to aid-geolocation of Sat Phones / GSM Phones via a silent calling to the phone.	Ready to fire.	
GATEWAY	Ability to artificially increase traffic to a website.	Ready to fire.	
GAMBIT	Deployable pocket-sized proxy server	In-development	

GESTATOR	amplification of a given message, normally video, on popular multimedia websites (Youtube).		
GLITTERBALL	Online Gaming Capabilities for Sensitive Operations. Currently Second Life.	In development.	
IMPERIAL BARGE	For connecting two target phone together in a call.	Tested.	
PITBULL	Capability, under development, enabling large scale delivery of a tailored message to users of Instant Messaging services.	In development.	
POISONED DAGGER	Effects against Gigatribe. Built by ICTR, deployed by JTRIG.		
PREDATORS FACE	Targeted Denial Of Service against Web Servers.		
ROLLING THUNDER	Distributed denial of service using P2P. Built by ICTR, deployed by JTRIG.		
SCARLET EMPEROR	Targeted denial of service against targets phones via call bombing.	Ready to fire.	
SCRAPHEAP CHALLENGE	Perfect spoofing of emails from Blackberry targets.	Ready to fire, but see constraints.	
SERPENTS TONGUE	for fax message broadcasting to multiple numbers.	In redevelopment.	

SILENT MOVIE	Targeted denial of service against SSH services.	Ready to fire.	
SILVERBLADE	Reporting of extremist material on DAILYMOTION.	Ready to fire.	
SILVERFOX	List provided to industry of live extremist material files hosted on FPU's.	Ready to fire.	
SILVERLORD	Disruption of video-based websites hosting extremist content through concerted target discovery and content removal.	Ready to fire.	
SKYSCRAPER	Production and dissemination of multimedia via the web in the course of information operations.	Ready to fire.	
STEALTH MOOSE	is a tool that will disrupt targets Window's machine. Logs of how long and when the effect is active.	Ready to fire (but see target restrictions).	
SUNBLOCK	Ability to deny functionality to send/ receive email or view material online.	Tested, but operational limitations.	
SWAMP DONKEY	is a tool that will silently locate all predefined types of file and encrypt them on a targets machine	Ready to fire (but see target restrictions).	
TORNADO ALLEY	is a delivery method (Excel Spreadsheet) that can silently extract and run an executable on a	Ready to fire (but see target restrictions).	

	target's machine.		
UNDERPASS	Change outcome of online polls (previously known as NUBILO).	In development.	
VIPERS TONGUE	is a tool that will silently Denial of Service calls on a Satellite Phone or a GSM Phone.	Ready to fire (but see target restrictions).	
WARPATH	Mass delivery of SMS messages to support an Information Operations campaign.	Ready to fire.	

## Work Flow Management

<b>Tool</b>	<b>Description</b>	<b>Contacts</b>
HOME PORTAL	A central hub for all JTRIG Cerberus Tools	JTRIG Software Developers
CYBER COMMAND CONSOLE	A centralised suite of tools, statistics and viewers for tracking current operations across the Cyber community.	JTRIG Software Developers
NAMEJACKER	A web service and admin console for the translation of usernames between networks. For use with gateways and other such technologies.	JTRIG Software Developers

## Analysis Tools

<b>Tool</b>	<b>Description</b>	<b>Contacts</b>
BABYLON	is a tool that bulk queries web	

	<p>mail addresses and verifies whether they can be signed up for. A green tick indicates that the address is currently in use. Verification can currently be done for Hotmail and Yahoo.</p>	
CRYOSTAT	<p>is a JTRIG tool that runs against data held in NEWPIN. It then displays this data in a chart to show links between targets.</p>	
ELATE	<p>is a suite of tools for monitoring target use of the UK auction site eBay (<a href="http://www.ebay.co.uk">www.ebay.co.uk</a>). These tools are hosted on an Internet server, and results are retrieved by encrypted email.</p>	
PRIMATE	<p>is a JTRIG tool that aims to provide the capability to identify trends in seized computer media data and metadata.</p>	
JEDI	<p>JTRIG will shortly be rolling out a JEDI pod to every desk of every member of an Intelligence Production Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficient and responsive to customer needs.</p>	
JILES	<p>is a JTRIG bespoke web browser.</p>	
MIDDLEMAN	<p>is a distributed real-time event aggregation, tip-off and tasking platform utilised by JTRIG as a middleware layer.</p>	
OUTWARD	<p>is a collection of DNS lookup, WHOIS Lookup and other network tools.</p>	

TANGLEFOOT	is a bulk search tool which queries a set of online resources. This allows analysts to quickly check the online presence of a target.	
SCREAMING EAGLE	is a tool that processes kismet data into geolocation information	
SLAMMER	is a data index and repository that provides analysts with the ability to query data collected from the Internet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysts etc.	

## Databases

Tool	Description	Contacts
BYSTANDER	Is a categorisation database accessed via web service.	JTRIG Software Developers
CONDUIT	is a database of C2C identifiers for Intelligence Community assets acting online, either under alias or in real name.	JTRIG Software Developers
NEWPIN	is a database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data.	JTRIG Software Developers
QUINCY	Is an enterprise level suite of tools for the exploitation of seized media.	[Tech Lead [CENSORED] Expert Users: ]

## Forensic Exploitation

<b>Tool</b>	<b>Description</b>	<b>Contacts</b>
BEARSCRAPE	can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box.	
SFL	The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution.	
Snoopy	is a tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK).	
MobileHoover	is a tool to extract data from field forensics' reports created by Celldek, Cellebrite, XRY, Snoopy and USIM detective. These reports are transposed into a Mewpm XML format to upload to Newpin.	
Nevis	is a tool developed by NTAC to search disk images for signs of possible Encryption products. CMA have further developed this tool to look for signs of Steganography.	123131

## Techniques

<b>Tool</b>	<b>Description</b>	<b>Contacts</b>
CHANGELING	Ability to spoof any email address and send email	

	under that identify	
HAVOCK (HAVLOCK?)	Real-time website cloning techniques allowing on-the-fly alterations.	
MIRAGE		
SHADOWCAT	End-to-End encrypted access to a VPS over SSH using the TOR network	
SPACE ROCKET	is a programme covering insertion of media into target networks. CRINKLE CUT is a tool developed by ICTR-CISA to enable JTRIG track images as part of SPACE ROCKET.	
RANA	is a system developed by ICTR-CISA providing CAPTCHA-solving via a web service on CERBERUS. This is intended for use by BUMPERCAR+ and possibly in future by SHORTFALL but anyone is welcome to use it.	
LUMP	A system that finds the avatar name from a SecondLife AgentID	
GURKHAS SWORD	Beaconed Microsoft Office Documents to elicit a targets IP address.	

## Shaping And Honeypots

Tool	Description	Contacts
DEADPOOL	URL shortening service	
HUSK	Secure one-on-one web based dead-drop messaging platform.	

LONGSHOT	File-upload and sharing website	
MOLTEN-MAGMA	CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle.	
NIGHTCRAWLER	Public online group against dodgy websites	
PISTRIX	Image hosting and sharing website	
WURTILIZER	Distribute a file to multiple file hosting websites.	